UNION / EMPLOYEE CONSULTATION COMMITTEE

AGENDA

Wednesday 12th March 2014 at 1100 hours in Chamber Suites 1 & 2, The Arc, Clowne

Item No.		Page No.(s)
	PART 1 – OPEN ITEMS	
1.	To receive apologies for absence, if any.	
2.	Election of Chair for meeting.	
3.	To note any urgent items of business which the Chairman has consented to being considered under the provisions of Section 100(B) 4 (b) of the Local Government Act 1972.	
4.	Members should declare the existence and nature of any personal or prejudicial interest in respect of:- a) any business on the agenda b) any urgent additional items to be considered c) any matters arising out of those items and, if appropriate, withdraw from the meeting at the relevant time.	
5.	To approve the Minutes of a meeting held on 11th December 2013.	3 to 8
6.	ICT Policies and Members ICT Charter.	9 to 135
7.	Pay Policy - Relief Central Control Operators.	136 to 138
8.	Sickness Absence/Occupational Health Statistics October to December 2013.	139 to 142
9.	Equalities Monitoring October to December 2013.	143 to 150

UNION/EMPLOYEE CONSULTATION COMMITTEE

Minutes of a meeting of the Union/Employee Consultation Committee of the Bolsover District Council held in Chamber Suite 1, The Arc, Clowne, on Wednesday 11th December 2013 at 1100 hours.

PRESENT:-

Council Representatives:-

Councillors Mrs P.M Bowmer, V.P. Mills, K. Reid and A.F Tomlinson.

Unison Representatives:-

J. Clayton, J. Wilmot, C. McKinney and K. Shillitto.

Unite Representatives:-

None attended.

Officers:-

T. Morrell (Senior HR Advisor, NEDDC), C. Ashton (HR Manager, NEDDC) and A. Bluff (Governance Officer).

0664. APOLOGIES

Apologies for absence were received on behalf of Councillors A.M. Syrett and E. Watts, S. Sambrooks (Unite) and A. Freeman (Unison Regional Office).

0665. ELECTION OF CHAIR FOR MEETING

Moved by J. Wilmot, seconded by K. Shillitto
RESOLVED that J. Clayton be elected as Chair for the meeting.

J. Clayton in the Chair

0666. APPOINTMENT OF VICE CHAIR

Moved by Councillor A.F. Tomlinson, seconded by Councillor K. Reid
RESOLVED that Councillor E. Watts be appointed as Vice Chair of the Committee for the ensuing year.

0667. URGENT ITEMS OF BUSINESS

Unison raised an urgent item of business for Committee to consider in relation to the Driving at Work Policy.

Unison agreed that the changes needed to be included in the policy but raised concern that these had not been presented through the correct channels for consultation.

A discussion took place.

The Senior HR Advisor, NEDDC, advised that she would look into this.

Moved by J. Wilmot, seconded by Councillor A. F. Tomlinson
RESOLVED that the Senior HR Advisor, NEDDC, look into why changes to the Driving Policy had not been presented correctly for consultation.

(Senior HR Advisor, NEDDC)

0668. DECLARATIONS OF INTEREST

There were no declarations of interest made.

0669. MINUTES – 14th MARCH 2013

Moved by K. Shillitto, seconded by J. Wilmot
RESOLVED that the minutes of a Union/Employee Consultation Committee meeting held on 14th March 2013 be approved as a correct record.

0670. SICKNESS ABSENCE / OCCUPATIONAL HEALTH STATISTICS JULYTO SEPTEMBER 2013

Members considered a report of the Assistant Director of Human Resources in relation to sickness absence/occupational health statistics for the period July 2013 to September 2013.

The target for sickness absence for July to September 2013 was 2 days per full time employee (FTE) and the outturn was 2.5 days per FTE. For comparison, the outturn figure for the same period in 2012 was 2.51 days per FTE.

A breakdown of the figures by department and by long term/short term sickness absence was attached to the report for Members' information.

The number of days lost due to long term sickness had reduced in 2013 by 134.5 days and the number of days lost due to short term sickness had reduced in 2013 by

41 days. It was noted that the average number of FTE employees had also reduced in 2013 by 67.87

The Occupation Health referral figure for July to September 2013 was 11 in comparison to 19 in the same period in 2012.

A breakdown of reasons for all long term sickness absence was detailed in the report, though an error in the table of figures was noted and Members were advised that reasons for absence under 'back/neck' had been included twice with two separate figures. The HR Manager, NEDDC, would check the figures and report back to Members.

It was noted that only 1 employee had declared stress as a reason for sickness absence.

A discussion took place regarding work related stress.

A Unison representative suggested that use of the Arc's gym facilities for staff could be looked at and also how the sickness absence policy was being adhered to. He also suggested that the policy be reviewed.

The Senior HR Advisor, NEDDC, replied that work related stress did not seem to be a particular issue at Bolsover but if the Unions felt that it was an issue, training for Managers and employees could be looked at. The sickness absence policy would also be one of the next policies to be reviewed. Councillor Tomlinson added that use of the gym facilities for staff was being looked at.

A query was raised in relation to the latest sickness absence figures for all Derbyshire authorities and the HR Manager, NEDDC, replied that this was about 8* days but would check the figure.

Moved by K. Shillitto, seconded by Councillor A.F. Tomlinson
RESOLVED that subject to clarification of the breakdown figures of reasons for all long term sickness absence, the report be received.

(Senior HR Advisor, NEDDC)

**Further to the UECC meeting on 11th of December 2013, in relation to sickness absence, we do not have data from all Derbyshire Authorities but of the 5 responses received for the year 2012/13, the average was 8.51 days per employee.*

0671. EQUALITIES MONITORING JANUARY TO MARCH 2013

Members considered a report in respect of Equalities Monitoring data for the period January to March 2013 on the Council's performance on equality issues in relation to its employment practices.

Moved by Councillor A.F. Tomlinson, seconded by K. Shillitto
RESOLVED that the report be received.

0672. EQUALITIES MONITORING APRIL TO JUNE 2013

Members considered a report in respect of Equalities Monitoring data for the period April to June 2013 on the Council's performance on equality issues in relation to its employment practices.

Moved by Councillor A.F. Tomlinson, seconded by K. Shillitto
RESOLVED that the report be received.

0673. EQUALITIES MONITORING JULY TO SEPTEMBER 2013

Members considered a report in respect of Equalities Monitoring data for the period July to September 2013 on the Council's performance on equality issues in relation to its employment practices.

Moved by Councillor A.F. Tomlinson, seconded by K. Shillitto
RESOLVED that the report be received.

0674. EXIT INFORMATION 1ST APRIL 2012 TO 31ST MARCH 2013

Members considered a report in respect of Exit information and a summary of primary reasons for permanent employees leaving the Authority for the period 1st April 2012 to 31st March 2013. The report also included comparisons for the same period in 2012.

A breakdown by department was included in the report along with a copy of the standard exit questionnaire for Members information.

Moved by Councillor K. Reid, seconded by K. Shillitto
RESOLVED that the report be received.

0675. DRAFT TIME OFF AND FACILITIES AGREEMENT FOR BOLSOVER DISTRICT COUNCIL

Members considered a report of the Senior HR Advisor, NEDDC, in respect of the draft Time Off and Facilities Agreement for Bolsover.

An amended version of the draft Agreement was circulated to the meeting and the Senior HR Advisor, NEDDC, explained that a reference was now included at the end of Point 9 in relation to the form at Appendix 1, which should be used to request time off. Also, point 14.3 now reflected the 21 days' notice requirement where it was previously referred to as notice of 'at least a few weeks'.

A short discussion took place and it was agreed that wording in the second sentence of the paragraph in the form (Appendix 1), be amended from; 'In the case of a union training course 21 days prior notice 'must' be given, ... to; 'In the case of a union training course 21 days prior notice 'preferably' be given.

Moved by Councillor K. Reid, seconded by J. Wilmot

RESOLVED that wording in the second sentence of the paragraph in the form (Appendix 1), be amended from; 'In the case of a union training course 21 days prior notice 'must' be given, ... to; 'In the case of a union training course 21 days prior notice 'preferably' be given.

A Unison representative raised concern with regard to point 18.3 and 18.4 of the Agreement under 'Disputes' in relation to a "matter being referred to UECC if an agreement could not be reached" and that this meant there was potentially a three month wait as UECC meetings were held quarterly.

A short discussion took place and it was agreed that if this circumstance arose then an extraordinary meeting of UECC could be arranged.

Moved by K. Shillitto, seconded by Councillor K. Reid

RECOMMENDED that subject to 'must' being changed to 'preferably' as per the recommendation above, the amended draft Time Off and Facilities Agreement for Bolsover be presented to Council for agreement and adoption.

(Senior HR Advisor, NEDDC/Governance Manager)

0676. SMOKE FREE POLICY

Members considered a report of the HR Manager, NEDDC, in respect of the Smoke Free Policy for Bolsover.

An amended version of the Smoke Free Policy was circulated to the meeting and the HR Manager, NEDDC, explained that under 'Policy Statement' at part 3, the last bullet point had been changed to read 'Smoking and the use of electronic cigarettes will not be permitted in Council buildings' rather than 'on Council grounds'. There was also another change to the reference at part 3 that the original policy was introduced in March 2008 and not October 2007.

Under part 5, 'Non Compliance', the HR Manager, NEDDC, explained that the Assistant Director of Public Health had advised that someone could not be requested to not smoke e-cigarettes in a private dwelling.

Further to a question raised by a Unison representative, it was clarified that not smoking 5 metres in front of any Council workplace meant any of the Council's buildings.

Unison raised that the Smoke Free Policy needed to be clear that it was about the image of the Council as well as peoples' health.

The HR Manager, NEDDC, advised that guidance had been sought and though e-cigarettes may not be as harmful, it was the image and reputation of people walking round the Council building smoking e-cigarettes.

A short discussion took place.

Members were further advised that the Smoke Free Policy had been adopted at NEDDC, and as this was a separate version for Bolsover, the NEDDC logo had been removed.

Moved by Councillor A.F. Tomlinson, seconded by Councillor K. Reid
RECOMMENDED that the Smoke Free Policy be presented to Council for agreement and adoption.

(HR Manager, NEDDC/Governance Manager)

0677. POLICY AND PROCEDURES FOR ORGANISATIONAL REVIEW

Members considered a report of the Senior HR Advisor, NEDDC, in respect of Policy and Procedures for Organisational Review.

North East Derbyshire District Council has had a policy for use in organisational reviews for some years which had recently been redrafted and updated. As Bolsover had no similar policy, and with the view of harmonising policies across both Councils wherever possible, it was proposed to forward the same draft policy to Council for adoption.

A discussion took place.

It was noted that although the content of the Policy was common to both BDC and NEDDC, reference to NEDDC would be taken out as this was a BDC Policy.

Unison noted that they would look forward to being involved as early as possible with the Chief Executive Officer when he is looking at organisational review.

Moved by K. Shillitto, seconded by Councillor V. Mills
RECOMMENDED that subject the reference to NEDDC being taken out of the Policy, the policy and Procedures for Organisational Review be presented to Council for agreement and adoption.

(Senior HR Advisor, NEDDC/Governance Manager)

The meeting concluded at 1215 hours.

Appendix 1

Bolsover District Council,
North East Derbyshire District Council
&
Rykneld Homes Ltd

INFORMATION SECURITY POLICY SUMMARY

CONTROL SHEET FOR Information Security Policy

Policy Details	**Comments / Confirmation** **(To be updated as the document progresses)**
Policy title	Information Security
Current status – i.e. first draft, version 2 or final version	Draft
Policy author(s)	Business Development Manager/ ICT Manager/ Senior Human Resources Advisor
Location of policy – i.e. L-drive, shared drive	Within IT data drive
Member route for approval	Scrutiny, Cabinet/Executive
Cabinet Member (if applicable)	Cllrs Rose Bowler(BDC) and Patricia Williams(NEDDC)
Equality Impact Assessment approval date	May 2013
Partnership involvement (if applicable)	
Final policy approval route i.e. Executive/ Council /Planning Committee	Executive/Cabinet
Date policy approved	
Date policy due for review (maximum three years)	2017
Date policy forwarded to Strategy and Performance (to include on Intranet and Internet if applicable to the public)	

Contents

1 Introduction

In order to ensure the continued delivery of services to our customers, Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. are making ever increasing use of Information and Communication Technology (ICT).

The information that the district councils and Rykneld Homes Ltd. holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

In order to maintain public confidence and ensure that the district councils and Rykneld Homes comply with relevant statutory legislation, it is vital that Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. maintain the highest standards of information security. As such, a number of policies are in place to maintain these high standards of information security; these are attached as appendices to this summary document. Members requirements are covered in the Members ICT Charter.

2 Scope

The policies applies to all users, the definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council , North East Derbyshire District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers, where they have access to ICT facilities.

These policies are produced in line with guidelines that are available as of September 2013. These include the Data Protection Act 1998 and standards such as the Public Services Network (PSN) Code of Connection. The policy will be updated in the event of changes to the Act and new guidelines published in respect to the PSN.

3 Principles

This document provides a summary of the information security policies developed by Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. The objective of these policies is to ensure the highest standards of information security are maintained across the district councils and Rykneld Homes at all times so that:

- The public and all users of the district councils and Rykneld Homes information systems are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- Customer and employee data is adequately protected and the risk of data protection breaches reduced.
- All legislative and regulatory requirements are met.
- The district councils and Rykneld Homes ICT equipment and facilities are used responsibly, securely and with integrity at all times.

4 Risks

Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd recognises that there are risks associated with users accessing and handling information in order to conduct official council or Rykneld Homes business. This policy aims to mitigate those risks.

Non-compliance with this policy could have a significant effect on the efficient operation of the council or Rykneld Homes and may result in financial loss and an inability to provide necessary services to our customers.

5 Information Security Policy

The detailed policies that are attached as appendices include:

- Email Policy (Appendix 1)
- Internet Acceptable Usage Policy (Appendix 2)
- Software Policy (Appendix 3)
- ICT Access Policy (Appendix 4)
- PSN Acceptable Usage Policy and Personal Commitment Statement (Appendix 5)
- Human Resources Information Security Standards (Appendix 6)
- Information Protection Policy (Appendix 7)
- Computer, Telephone and Desk Use Policy (Appendix 8)
- Remote Working Policy (Appendix 9)
- Removable Media Policy (Appendix 10)
- Information Security Incident Management Policy (Appendix 11)

- IT Infrastructure Policy (Appendix 12)

A summary of the relevant points as they apply to all users is included below, although employees should always refer to the relevant appendix for more detailed policy information.

5.1 Email (Appendix 1)

- The use of email facilities will be permitted only by users that have been specifically designated as authorised users for that purpose, received appropriate training and have confirmed in writing that they accept and agree to abide by the terms of this policy.

- All emails sent via the Government Connect Secure Extranet (GCSx) carrying PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) content and/or attachments must be of the format "@<council>.gcsx.gov.uk". A full explanation of the National Protective Marking scheme is available on the Council Intranet.
- Non-work email accounts **must not** be used to conduct or support official business.
- Users must ensure that any emails containing sensitive information must be sent from an official council email and be protected accordingly.
- All official external e-mail must carry the official council disclaimer.
- Under no circumstances should users communicate material (either internally or

externally), which is defamatory, obscene, or does not comply with the equality legislation.
- Forwarding of email to non-work email accounts must be considered carefully to prevent personal data, PROTECT, RESTRICTED or OFFICIAL material being transmitted inappropriately. Why are we allowing this?
- The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd business should be considered to be an official communication from the council or Rykneld Homes.

- Whilst respecting the privacy of authorised users, Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd reserves the right, with written approval from an appropriate Director or the Human Resources Manager, to monitor emails sent within the councils & Rykneld Homes email system (including personal emails) and to access mailboxes and private directories without further notifying the individual concerned that the right is being exercised.

- Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the councils or Rykneld Homes ICT systems.

- It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

5.2 Internet Acceptable Usage (Appendix 2)

- Internet use is monitored by the district councils and Rykneld Homes.
- Users must familiarise themselves with the detail, essence and spirit of this policy before using the Internet facility provided.
- At the discretion of line manager, and provided it does not interfere with your work, the councils and Rykneld Homes permits personal use of the Internet in your own time (for example during your lunch-break).
- Users are responsible for ensuring the security of their Internet account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.
- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.

Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

5.3 Software (Appendix 3)

- All software acquired must be purchased through the ICT Section.
- Under no circumstances should personal or unsolicited software be loaded onto a council or Rykneld Homes machine.
- Every piece of software is required to have a licence and the councils and Rykneld Homes will not condone the use of any software that does not have a licence.
- Unauthorised changes to software **must not** be made.

- Users are not permitted to bring software from home (or any other external source) and load it onto councils or Rykneld Homes computers.
- Users **must not** attempt to disable or reconfigure the personal firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

5.4 ICT Access (Appendix 4)

- All users must use strong passwords, see appendix 4 for details.
- Passwords must be protected at all times and must be changed at least every 60 days.
- It is a users responsibility to prevent their user ID and password being used to gain unauthorised access to the Councils or Rykneld Homes systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Councils or Rykneld Homes network without permission from the ICT Manager.
- Partners or 3rd party suppliers must contact the ICT Section before connecting to the Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. network.

5.5 PSN Acceptable Usage and Personal Commitment Statement (Appendix 5)

This applies mainly to North East Derbyshire and Bolsover but Rykneld Homes also have a need to send and receive secure communications.

- Each PSN (Public Services Network) user must read, understand and sign the 'Personal Commitment Statement' to verify they have read and accepted the policy.

5.6 Human Resources Information Security Standards (Appendix 6)

- Every ICT user must be aware of, and understand, this policy, and the policies detailed in the appendices.

5.7 Information Protection Policy (Appendix 7)

- The councils and Rykneld Homes must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG(Her Majesty's Government) Security Policy Framework (SPF).
- Information up to RESTRICTED or OFFICIAL(subject to descriptor)sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until their Line Manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

- PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) information **must not** be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) classified information to any external organisation is also **prohibited**, unless via the GCSx email.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) material.
- The disclosure of PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) classified information in any way other than via GCSx email is a disciplinary offence.

5.8 Computer, Telephone and Desk Use (Appendix 8)

- Users must adhere to North East Derbyshire District Council, Bolsover District Council and Rykneld Homes Ltd. Computer, Telephone and Desk Use Policy at all times.
- Users should aim to maintain a clear desk at all times.
- North East Derbyshire District Council, Bolsover District Council and Rykneld Homes Ltd. PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

5.9 Remote Working (Appendix 9)

- It is the users responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices and not emailing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information to a non-council or non Rykneld Homes email address.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- All PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) data held on portable computer devices must be encrypted.

5.10 Removable Media (Appendix 10)

- The use of all removable media devices is prohibited unless a business case is agreed, security training has been given, and agreement signed to this effect.
- Any removable media device that has not been supplied by IT **must not** be used.
- All data stored on removable media devices **must** be encrypted where possible, and personal data must not be stored on devices that are not encrypted. Only data that is authorised and necessary to be transferred should be saved on to the removable media device. N.B. Data that has been deleted can still be retrieved.
- Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.
- Damaged or faulty removable media devices must not be used.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be taken to the IT section for secure disposal.

- Users should be aware of their responsibilities in regard to the Data Protection Act and report any suspected breaches.

5.11 Information Security Incident Management (Appendix 11)

- All users should report any incidents or suspected incidents immediately by contacting the ICT Section.
- Anonymity when reporting an incident can be maintained if desired.
- If an incident requires information to be collected for an investigation, strict rules must be adhered to. Internal Audit should be contacted for guidance.
- Users should be aware of their responsibilities in regard to the Data Protection Act and report any suspected breaches.

5.12 ICT Infrastructure Security (Appendix 12)

- PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information, and equipment used to store and process this information, must be **stored** securely.
- Desktop PCs should not have data stored on the local hard drive. This may require training and support from ICT for some users to migrate their files to network drives.
- Non-electronic information must be assigned an owner and a classification. PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information must have appropriate information security controls in place to protect it.
- Users should be aware of their responsibilities in regard to the Data Protection Act and report any suspected breaches.
- Desktop PCs should not have data stored on the local hard drive.
- Equipment that is to be reused or disposed of must be returned to ICT to have all of its **data and software erased / destroyed**.

5.13 Data Protection

- At Bolsover and North East Derbyshire the Strategy and Performance department ensures that every member of users is aware of, and understands, their responsibilities under the Data Protection Act 1998 and other relevant legislation. At Rykneld Homes this is undertaken by their Business Development Manager.
- Adherence to this policy and the specific policies listed supports compliance with the Data Protection Act 1998 and reduces the risk of data protection breaches.

6 Responsibility for Implementation

The following table identifies who within North East Derbyshire District Council, Bolsover District Council and Rykneld Homes Ltd. is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.

- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Manager
Accountable	Section 151 Officer
Consulted	Human Resources, Data Protection Officer, Scrutiny, Consultative groups (UECG, JCG).
Informed	All Bolsover District Council , North East Derbyshire District Council or Rykneld Homes Ltd's Employees, all users as defined in the scope

7 Policy Compliance

All users will be required to undertake an ICT Induction and sign a declaration confirming they have received the training and confirm they will abide by the ICT Policies. A copy of this form can be seen in Appendix 13.

If any user is found to have breached this, or any policy contained within the Appendices attached, they will be subject to North East District Council, Bolsover District Council or Rykneld Homes Ltd. disciplinary procedure, as appropriate. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this, or any policy contained within the Appendices attached, or how they may apply to you, seek advice from your line manager.

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd's
- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information Security Manager or their department or service manager.

8 Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would cause significant damage to North East Derbyshire District Council, Bolsover District Council & Rykneld Homes Ltd's reputation or ability to operate
- If an emergency, within the context of the emergency plan, arises

In such cases, the user concerned must take the following action:

- Ensure that a North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd's manager is aware of the situation and the action to be taken.
- Ensure that the situation and the actions taken are recorded in as much detail as possible and reported to the ICT Service Desk.
- Ensure that the situation is reported to the Information Security Manager as soon as possible.
- If complying with the policy would breach Health and Safety.
- Failure to take these steps may result in disciplinary action.

In addition, ICT maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd will take no disciplinary action in relation to known, authorised exceptions to the information security management system.

This policy will be included within the North East Derbyshire District Council, Bolsover District Council & Rykneld Homes Ltd's Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.

9 Glossary of terms

Public Services Network(PSN) - This is a secure wide area network (WAN) that allows access to Central Government systems, secure data transfer, secure email and accredited solutions provided by public sector organisations and accredited 3rd parties. At present this includes gcsx secure email, CIS(Benefits), TellUsOnce and Electoral Registration systems. The scope of the PSN network covers local authorities, central government departments, National Health Service, the Criminal Justice Extranet and the Police National Network.

Government Security Classifications - a marking scheme of information assets as used by the UK Government. A new marking classification comes into effect from April 2nd 2014. Details of this scheme can be found via https://www.gov.uk/government/publications/government-security-classifications and the new marking classification guidelines can be found in Appendix A. Documents marked under the old marking scheme will still be in circulation and details of the scheme are found in Appendix B. There is no direct correlation between the two schemes but we should only ever receive documents marked 'UNCLASSIFIED', 'RESTRICT' or 'PROTECT' under the old scheme or 'OFFICIAL' under the new 20014 scheme. The latter may have additional descriptors such as '-SENSITIVE', '-COMMERCIAL' or '-PERSONAL'.

10 Contact Information

At the time of publication of this policy

the ***ICT Servicedesk*** is available on :-

- Self Service portal > http://sworksrv.ne-derbyshire.gov.uk/sw/selfservice/
- Email :- servicedesk@ne-derbyshire.gov.uk
- Telephone :- **3001** or 01246 21**7103**
-
- Monday to Friday 08:00am – 5:30pm

For incidents outside of these hours please contact the Information Security Manager who is the IT Manager.

APPENDIX 1 - E-MAIL POLICY

1. Introduction

Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd. will ensure all users of council and Rykneld Homes email facilities are aware of the acceptable use of such facilities.

The Policy establishes a framework within which users of Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd's email facilities can apply self-regulation to their use of email as a communication and recording tool.

2. Scope

This policy covers all email systems and facilities that are provided by Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd for the purpose of conducting and supporting official business activity through the , Bolsover District Council , North East Derbyshire District Council or Rykneld Homes Ltd's network infrastructure and all stand alone and portable computer devices.

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers, who have been designated as authorised users of email facilities.

The use of email facilities will be permitted only by users that have been specifically designated as authorised users for that purpose, received appropriate training and have confirmed in writing that they accept and agree to abide by the terms of this policy.

The use of email facilities by users that have not been authorised for that purpose will be regarded as a disciplinary offence.

The policies are based on industry good practice and intend to satisfy the requirements set out by the Government Connect Secure Extranet Code of Connection (CoCo).

References to PROTECT, RESTRICTED and OFFICIAL and guidance on assessing and handling such information are explained in the PSN acceptable usage policy within the national protective marking scheme and Government Security Classification scheme.

3. Email Policy

3.1 Email as Records

- All emails that are used to conduct or support thecouncils business must be sent using a "@<council>.gov.uk" address. All emails that are used to conduct or support official Rykneld Homes Ltd business must be sent using a "@rykneldhomes.org.uk" address.
- All emails sent via the Government Connect Secure Extranet (GCSx) carrying PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) content and/or attachments must be of the format "@council.gcsx.gov.uk".
- Non-work email accounts **must not** be used to conduct or support official business.
- Users must ensure that any emails containing sensitive information must be sent from an official council email and be protected accordingly.
- All official external e-mail must carry the official council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with equality legislation.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for communicating PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) material.
- Where GCSx email is **not** available to connect the sender and receiver of the email message, and information classified as PROTECT OR OFFICAL(subject to descriptor) is being transferred, encryption **should** be used for all content and/or attachments that contain that classification. The ICT Service Desk will advise on options available.
- Where GCSx email is **not** available to connect the sender and receiver of the email message, and information classified as RESTRICTED or OFFICAL(subject to descriptor) is being transferred, encryption **must** be used for all content and/or attachments that contain that classification. The ICT Service Desk will advise on options available.
- Emails carrying PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) contents and/or attachments must be labelled to highlight the sensitivity and value that the information has to the data owner. This will be in the format of the Subject Header containing the label "PROTECT", "RESTRICTED" or "OFFICIAL"(with appropriate descriptor) as appropriate.
- Automatic forwarding of email must be considered carefully to prevent PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) material being forwarded inappropriately.

Non-work email accounts **must not** be used to conduct or support official Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd business. Users must ensure that any emails containing sensitive information must be sent from an official council email. Any Bolsover District Council or North East Derbyshire District Council emails containing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information must be sent from a GCSx email. All emails that represent aspects of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd business or Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd administrative arrangements are the property of Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd., as appropriate, and not of any individual employee.

Emails held on North East Derbyshire District Council, Bolsover District Council & Rykneld Homes Ltd equipment are considered to be part of the corporate record and email also provides a record of user's activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd business should be considered to be an official communication from the council or Rykneld Homes. In order to ensure that Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd is protected adequately from misuse of e-mail, the following controls will be exercised:

i. It is a condition of acceptance of this policy that users comply with the instructions given during the email training sessions.
ii. All official external e-mail must carry the following disclaimer:

> *"Disclaimer*
>
> *This email is confidential, may be legally privileged and contain personal views that are not the views of* ***Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd (amend as required).***
>
> *It is intended solely for the addressee. If this email was sent in error please notify the sender, delete the email and do not disclose, copy, distribute, or rely on it. Under the Data Protection Act 1998 and the Freedom of Information Act 2000 the contents of this email may be disclosed.*
>
> *This message and attached files have been virus scanned. Attachments are opened at your own risk."*

Whilst respecting the privacy of authorised users, Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd reserves the right, with written approval from an appropriate Director or the Human Resources Manager, to monitor emails sent within the councils & Rykneld Homes email system (including personal emails) and to access mailboxes and private directories without further notifying the individual concerned that the right is being exercised.

The councils and Rykneld Homes may exercise this right, with written approval from an appropriate Director or the Human Resources Manager and in accordance with the Data Protection Policy, in order to establish facts relevant to the councils & Rykneld Homes' business and to comply with:

- regulatory practices or procedures,
- to prevent or detect crime,
- to ensure compliance with Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd policies,
- to investigate or detect unauthorised uses of the system or to ensure the effective operation of the system (e.g. to check if viruses are being transmitted).
- to ensure critical work or urgent items can be actioned.

In these circumstances you do not have a right to privacy when using the Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd's information systems or in relation to any communication generated, received or stored on the Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd's information systems.

These actions will be supervised by the Information Security Manager.

Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the councils or Rykneld Homes ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the appropriate Data Protection Officer.

3.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information or of communicating in the particular circumstances.

All emails sent to conduct or support official Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd business must comply with corporate communications standards. Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd's Communications and Operation Management Policy must be applied to email communications.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd's reputation or its relationship with customers, clients or business partners.

When sending emails internally or externally the user should exercise due care in selecting the recipients to send the communication to. This is particularly important when sending personal and sensitive data.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) material concerning the activities of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste users effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, marital status, disability, political, religion or belief, maternity or paternity, civil partnership, gender reassignment or sexual orientation.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd into disrepute.

3.3 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that they delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd systems or facilities.

3.4 Mail Box Size

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addresses is discouraged.

Users are provided with a limited mail box size of 120mb to reduce problems associated with server capacity. Users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 5mb in size.

3.5 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd:

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

Monitoring of content will only be undertaken by users specifically authorised for that purpose. These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

a. Establishing the existence of facts relevant to the business, client, supplier and related matters.

b. Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
c. Preventing or detecting crime.
d. Investigating or detecting unauthorised use of email facilities.
e. Ensuring effective operation of email facilities.
f. Determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact the Information Security Manager. Designated users in the ICT Section can investigate and provide evidence and audit trails of access to systems. The ICT Section will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. If this is the case Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd may exercise this right, with written approval from an appropriate Director or Assistant Director or the Human Resources Manager and in accordance with the Data Protection Policy. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the employee. Managers must only open emails which are relevant.

3.6 Categorisation of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the HMG Security Policy Framework (SPF). The marking classification will determine how the email, and the information contained within it, should be protected and who should be allowed access to it.

The SPF requires information to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependent on this scheme.

From April 2014 the classifications are:

- OFFICAL
- SECRET
- TOP SECRET

The classifications pre April 2014 may remain in circulation and are:

- Unclassified.
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.

- TOP SECRET.

Information up to RESTRICTED or OFFICIAL sent via GCSx must be marked appropriately using the SPF guidance.

We should never receive or mark emails with the classifications SECRET, TOP SECRET or CONFIDENTIAL.

You should refer to the Information Protection Policy for full details on the application of information classification.

3.7 Security

Emails sent between:

ne-derbyshire.gov.uk and ne-derbyshire.gov.uk

ne-derbyshire.gov.uk and rykneldhomes.org.uk

rykneldhomes.org.uk and rykneldhomes.org.uk

rykneldhomes.org.uk and ne-derbyshire.gov.uk

bolsover.gov.uk and bolsover.gov.uk

addresses are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, North East Derbyshire District Council or Bolsover District Council PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) material must not be sent via email outside a closed network, unless via the GCSx email.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) material.

Where GCSx email is not available to connect the sender and receiver of the email message, and information classified as PROTECT is being transferred, encryption should be used for all content and/or attachments that contain that classification.

Where GCSx email is not available to connect the sender and receiver of the email message, and information classified as RESTRICTED is being transferred, encryption must be used for all content and/or attachments that contain that classification.

Emails carrying PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) contents and/or attachments must be labelled to highlight the sensitivity and value that the information has to the data owner. This will be in the format of the Subject Header containing the label “PROTECT”, “RESTRICTED” or “OFFICAL” (with appropriate descriptor) as appropriate.

All users that require access to GCSx email must read, understand and sign the PSN Acceptable Usage Policy and Personal Commitment Statement.

3.8 Confidentiality

All users are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data (customers and employees). If any user is unsure of whether they should pass on information, they should consult the relevant Data Protection Officer.

Users must make every effort to ensure that the confidentiality of email is appropriately maintained. Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd.

Care should be taken when addressing all emails, but particularly where they include PROTECT, RESTRICTED or OFFICIAL information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent PROTECT, RESTRICTED or OFFICIAL material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the ICT Servicedesk in the first instance.

The automatic forwarding of a GCSx email to a lower classification email address (i.e. a standard .gov.uk email) contradicts national guidelines and is therefore not acceptable.

3.9 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the ICT section.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer

which they use to access North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd facilities.
- Must not forward virus warnings other than to the ICT Servicedesk.
- Must report any suspected files to the ICT Servicedesk.

In addition, the councils and Rykneld Homes will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the councils or Rykneld Homes could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

APPENDIX 2 - INTERNET ACCEPTABLE USAGE POLICY

1. Introduction

Bolsover District Council, North East Derbyshire District Council, and Rykneld Homes Ltd. provide many and diverse Information and Communications Technology ("ICT") services, tools and equipment to employees to be used in the course of their work, including computers, laptops, telephones, internet and email.

The internet has become a fundamental tool which the councils and Rykneld Homes use for research and education purposes. Internally, the councils and Rykneld Homes have also developed Intranet sites (eRic, NEDi, and RYKi) to aid the dissemination of relevant information amongst employees.

The councils and Rykneld Homes support information and communications resources which will enhance the business and service environment. However, with access to computers and people all over the world via ICT comes the availability of material that may not be considered of value in the context of the councils and Rykneld Homes setting. Additionally, as with any resource, there is the possibility of misuse. Accordingly, the councils and Rykneld Homes needs to set guidelines for the use of ICT and, where appropriate, to monitor its use.

However, even with the guidelines, the councils and Rykneld Homes cannot prevent the possibility that some users may access material, even inadvertently, that is not consistent with the policies of the councils or Rykneld Homes or in line with the normal duties and responsibilities of the user.

2. Scope

All information, whether electronic or paper based, relating to our customers, suppliers and business operations should be treated in line with (a) the councils and Rykneld Homes Code of Conduct for Members and Officers, (b) relevant policies and (c) relevant legislation.

2.1 Legislation:

Copyright, Designs and Patents Act 1988 – downloading, copying, processing or distributing information from the internet may be an infringement of copyright or other intellectual property rights.

Data Protection Act 1998 – care should be taken in the collection, processing or disclosure of any personal data and all personal data should be processed within the principles of the Act.

Human Rights Act 1998 – The HRA provides for the privacy of personal correspondence and the protection of that privacy while at work. Monitoring unless notified and done properly may infringe these rights

Freedom of Information Act 2000 – all recorded information is potentially disclosable under the Act, including all expressions of fact, intent and opinion. If a request for information is made, the Act prohibits destruction of the information until it is given out in response to the request. Please also see the councils and Rykneld Homes guidelines on retention of information.

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of North East Derbyshire District Council, Bolsover District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who make use of the internet.

3. Principles

This policy sets out the rules by which Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. expects users to employ the ICT services and equipment in order to carry out their duties in a sensible, professional and lawful manner in accordance with law and the councils and Rykneld Homes Code of Conduct for Officers.

The guidelines aim to set out the councils and Rykneld Homes policy on the use and monitoring of ICT and seek to strike a balance between users' right to privacy and the councils and Rykneld Homes responsibility to ensure appropriate use of ICT.

Failure to comply with these guidelines may be viewed as a disciplinary matter and may, therefore, be subject to the councils and Rykneld Homes agreed Disciplinary Procedure and Code of Practice.

It is intended that from time to time, as is required by changes to legislation, technology or councils or Rykneld Homes policy, these Guidelines will be reviewed. Any changes made will be agreed both by the trades unions and members and the changes communicated to the users who have signed the original document. By signing the agreement users are deemed to accept any revisions to this policy that are communicated to them.

Non-compliance with this policy could have a significant effect on the efficient operation of the councils and Rykneld Homes and may result in financial loss and an inability to provide necessary services to our customers.

4. What is the Purpose of Providing the Internet Service?

4.1 General guidelines on use of the internet

Use of the Internet is available at your line manager's discretion. In general, users shall only use the Internet for official purposes, eg access to and the provision of information, research, electronic commerce. Use of information from the Internet shall be directly related to the official duties of the user, or the councils or Rykneld Homes as a whole. All information downloaded from the Internet shall be related to the duties and tasks of the user. However, reasonable personal use is permitted within a users own time at the discretion of their line manager.

Where there is public access to the Internet provided by the councils or Rykneld Homes and a member of the public misuses this provision, it will not be deemed to be the responsibility of any employee present at the time. However, the employee should report this incident as a breach of security to ICT.

Any information distributed or released by users by way of the Internet is subject to the councils or Rykneld Homes guidance on the release of information and shall, prior to such distribution, be approved by the relevant management procedures.

Any proposed links from the councils or Rykneld Homes Internet sites to the other Internet sites must first be authorised by your Director.

Users must be aware that the quality and accuracy of information available on the Internet is variable. It is the responsibility of the individual user to judge whether the information obtained is satisfactory for the purpose for which it will be used, and, if appropriate, steps should be taken to verify this information independently.

Where the Internet is being accessed by employees via a mobile device (laptop or tablet, or smartphone) from an internet connection which is not covered by the councils or Rykneld Homes internet filtering software, the same guidelines on appropriate use of the Internet apply and extra care must be taken not to visit sites which would be deemed unsuitable.

Virus protection software will be installed and configured on all councils and Rykneld Homes computer equipment. The configuration of these must not be altered and is updated regularly. Where home computer facilities are used for work purposes it is the individual's responsibility to ensure that anti virus software is installed and is updated regularly. Care must be taken with mobile storage devices to ensure that files stored on these devices do not become infected.

No personal ICT equipment may be attached to the councils or Rykneld Homes network without the permission of the ICT Manager.

Only memory sticks provided by the council or Rykneld Homes may be used.

4.2 Specific Guidelines on Use of the Internet

- Software, including MP3 files, must not be downloaded from the Internet by users without the advice and permission of ICT personnel.
- When participating in newsgroups or mailing lists, users may offer information and advice to others if it is appropriate to their official duties or tasks or if the benefit to be gained by the councils or Rykneld Homes represents a reasonable return in terms of the effort involved.
- Employees must not take part in discussions on political matters via the Internet unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited trade union representative.
- Users must not use their access to the Internet for their own private business purposes.

- Orders for goods purchased for council or Rykneld Homes purposes must not be placed by way of the Internet without the employee having first obtained approval from their line manager, having authorised the purchase in the normal departmental manner and having complied with the council's or Rykneld Homes Contract Standing Orders and Financial Regulations.
- Users must not use the councils or Rykneld Homes Internet facility for the purpose of gambling.
- Users must not break or attempt to break any system security controls placed on their Internet Account.
- Users must not intentionally access or transmit computer viruses or software programs used to trigger these.
- Users must not intentionally access or transmit information which is obscene, sexually explicit, racist or defamatory or which depicts violent or criminal acts or otherwise represents values that are contrary to councils or Rykneld Homes policy.
- Employees must not intentionally access or transmit information of a political nature unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited trade union representative.
- Users must not knowingly break the law.
- If an Internet site containing unsuitable material e.g. of an obscene nature is inadvertently accessed by a user, this must be immediately reported to ICT as a security breach.
- If material is inadvertently accessed which is believed to contain a computer virus, the user must immediately break the connection to the Internet and contact ICT for advice and assistance.
- Users must not copy information originating from others and re-post it without the permission of or acknowledgement to the original source.

5. Personal Use of the Internet Service

Any reasonable personal use of the councils and Rykneld Homes ICT services and equipment must comply with the councils and Rykneld Homes Code of Conduct for Officers and Members. Reasonable personal use of such services and equipment:-

- Must not be carried out in works time
- Must not interfere with the performance of your duties.
- Must not take priority over your work responsibilities
- Must not result in the councils or Rykneld Homes incurring expense
- Must not have a negative impact on the councils or Rykneld Homes.
- Must be lawful and in accordance with council and Rykneld Homes Policy and with the guidelines as set out in this document.

Where reasonable personal use is referred to in this document, this section applies.

Reasonable personal use of the councils or Rykneld Homes internet service is permitted only in the employee's own time (i.e. before clocking on, or after clocking off in accordance with the appropriate flexitime Scheme).

6. Internet Account Management, Security and Monitoring

6.1 Monitoring and Reporting Internet Use

All access to the Internet is automatically logged against an identifier unique to the PC of the user, is recorded and may be monitored by the councils and Rykneld Homes. This monitoring will be for the prevention and detection of unauthorised use of the councils and Rykneld Homes communication systems.

Auditable statistics are kept within ICT of all council and Rykneld Homes Internet access.

Line managers are able to access details of sites visited by employees and the time spent accessing the internet. Such reporting is not provided on a set basis, but will be available to managers in the normal course of an investigation into inappropriate or prolonged use of the Internet by a user.

The councils and Rykneld Homes ICT actively monitors access to inappropriate sites via the Internet security software. Any 'irregularities' encountered in this process are reported to the line manager of an employee in accordance with the Councils or Rykneld Homes Code of Conduct.

For councils and Rykneld Homes, in the case of an investigation requiring to be carried out into the use of Internet access by a user, the relevant authority (this will be the line manager and/or Human Resources in the cases of an employee) will contact the ICT section who will access the necessary monitored information and provide a report of this to the relevant authority.

Internet filtering software is used to block access to sites which have been deemed unacceptable. In certain cases, where authorised by a line manager, users in specific

posts may be allowed access to sites normally blocked to users where access to sites is required or helpful in the undertaking of the duties of the post.

The councils and Rykneld Homes will provide a secure logon-id and password facility for your Internet account. The IT Section is responsible for the technical management of this account. You are responsible for the security provided by your Internet account logon-id and password. Only you should know your log-on id and password and you should be the only person who uses your Internet account.

7. Things You Must Not Do

Access to the following categories of websites is currently blocked using a URL filtering system:

- Adult/Sexual/Pornographic
- Alcohol and Tobacco
- Blogs, Forums and Web chat
- Drugs/Gambling
- Games/Downloads
- Hacking/Peer-to-peer
- Illegal/Criminal activity
- Religious extremism
- Offensive/Intolerance
- Hate and Discrimination
- Mobile Phones/Ringtones
- Personal Dating
- Some Search Engines
- Spyware/Spam URL's
- Violence and Weapons
- Suicide

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Run a private business.
- Download any software that does not comply with the councils and Rykneld Homes Software Policy.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other councils and Rykneld Homes policies.

In particular you are reminded that Powerpoint presentations with unsuitable images should not be downloaded.

8. Your Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the councils or Rykneld Homes Internet facility within the terms described herein.
- Read and abide by the following related policies:
    - Email Policy. (see Appendix 1)
    - Software Policy. (see Appendix 3)
    - IT Security Policy.(see Summary)

9. Whom Should I Ask if I Have Any Questions?

In the first instance you should refer questions about this policy to your Line Manager who will refer you to an appropriate contact. You should refer technical queries about the councils or Rykneld Homes Internet service to the IT Manager.

APPENDIX 3 - SOFTWARE POLICY

1. Introduction

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. will ensure the acceptable use of software by all users of the councils and Rykneld Homes computer equipment or information systems.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who make use of ICT equipment.

3. Principles

This policy sets out the rules by which Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. expects users to employ the ICT services and equipment in order to carry out their duties in a sensible, professional and lawful manner in accordance with law and the councils and Rykneld Homes Code of Conduct for Officers.

4. Software Policy

This policy should be applied at all times whenever using the councils or Rykneld Homes computer equipment or Information systems.

4.1 Software Acquisition

All software acquired by Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. must be purchased through the ICT Section. Software may not be purchased through user corporate credit cards, petty cash, travel or entertainment budgets. Software acquisition channels are restricted to ensure that Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. has a complete record of all software that has been purchased for Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a councils or Rykneld Homes machine as there is a serious risk of introducing a virus.

4.2 Software Registration

The councils and Rykneld Homes use software in all aspects of its business to support the work carried out by its employees. In all instances every piece of software is required to have a licence and the councils and Rykneld Homes will not condone the use of any software that does not have a licence.

Software must be registered in the name of Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd, whichever is appropriate and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The ICT Section maintains a register of all Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. software and will keep a library of software licenses. The register must contain:

a) The title and publisher of the software.
b) The date and source of the software acquisition.
c) The location of each installation as well as the serial number of the hardware on which each copy of the software is installed.
d) The existence and location of back-up copies.
e) The software product's serial number.
f) Details and duration of support arrangements for software upgrades.

Software on local area networks or multiple machines shall only be used in accordance with the licence agreement.

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. holds licences for the use of a variety of software products on all councils and Rykneld Homes Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer.

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

4.3 Software Installation

Software must only be installed by the ICT Section once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by the ICT Section.

Software may not be used unless approved by the ICT Manager, or their nominated representative.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto the councils or Rykneld Homes systems without prior approval from ICT Section

4.4 Software Development

All software, systems and data development for the councils and Rykneld Homes is to be used only for the purposes of the councils and Rykneld Homes.

Software must not be changed or altered by any user unless there is a clear business need. All changes to software should be authorised before the change is implemented. A full procedure should be in place and should include, but not be limited to, the following steps:

1. Change requests affecting a software asset should be approved by the software asset's owner.
2. All change requests should consider whether the change is likely to affect existing security arrangements and these should then be approved.
3. A record should be maintained of agreed authorisation levels.
4. A record should also be maintained of all changes made to software.
5. Changes to software that have to be made before the authorisation can be granted should be controlled.

4.5 Personal Computer Equipment

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd computers are the purchasing Council or Rykneld Homes owned assets and must be kept both software legal and virus free. Only software acquired through the procedures outlined above may be used on Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. machines. Users are not permitted to bring software from home (or any other external source) and load it onto Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. computers. Generally, council or Rykneld Home owned software cannot be taken home and loaded on a user's home computer if it also resides on a Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. computer. If a user needs to use software at home, they should purchase a separate package and record it as a council or Rykneld Homes owned asset in the software register.

4.6 Software Misuse

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. will ensure that Personal Firewalls are installed where appropriate. Users **must not** attempt to disable or reconfigure the Personal Firewall software.

It is the responsibility of all councils and Rykneld Homes users to report any known software misuse to the ICT Section.

According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. user who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under

the circumstances. Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. does not condone the illegal duplication of software and will not tolerate it.

APPENDIX 4 - ICT ACCESS POLICY

1. Introduction

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of North East Derbyshire District Council, Bolsover District Council and Rykneld Homes Ltd. which must be managed with care. All information has a value to the councils and Rykneld Homes. However, not all of this information has an equal value or requires the same level of protection.

Access control r**u**les and procedures are required to regulate who can access Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. information in any format, and on any device.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who access ICT equipment.

3. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

4. Applying the Policy - Passwords

4.1 Choosing passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words that may be present in a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters.
- Contain a mix of alpha and numeric, with at least one digit
- Contain a mix of upper and lower case with at least one upper case character

4.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your user name within the password.
- Do not use the same password to access Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd.
- Do not use the same password for systems inside and outside of work.

4.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 60 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the ICT Section.

Users **must not** reuse the same password within 20 password changes.

5. System Administration Standards

The password administration process for individual Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. systems is well-documented and available to designated individuals.

All Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users- i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

6. Applying the Policy – Employee Access

6.1 User Registration

A request for access to the council's computer systems must first be submitted to the ICT section for approval. Applications for access must only be submitted if approval has been gained from your line manager.

When a user leaves the councils or Rykneld Homes, their access to computer systems and data must be suspended at the close of business on the user's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the ICT Section.

6.2 User Responsibilities

It is a users responsibility to prevent their user ID and password being used to gain unauthorised access to the councils and Rykneld Homes systems by:

- Following the password policy and statements outlined above.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the ICT Section of any changes to their role and access requirements.

6.3 Network Access Control

The use of modems on non-council or Rykneld Homes owned PC's connected to the councils or Rykneld Homes network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the ICT Section before connecting any equipment to the councils or Rykneld Homes network.

7. Users Authentication for External Connections

Where remote access to the Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. network is required, an application must be made to the ICT Section. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a biometric device or authentication token. For further information please refer to the Remote Working Policy (Appendix 9).

7.1 Supplier's Remote Access to the Network

Partner agencies or 3rd party suppliers must not be given details of how to access the councils or Rykneld Homes network without permission from the ICT Section. Any changes to supplier's connections must be immediately sent to the ICT Section so that access can be updated or ceased. All permissions and access methods must be controlled by the ICT Section.

Partners or 3rd party suppliers must contact the ICT Section before connecting to the Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. network and a log of activity must be maintained. Remote access software must be disabled when not in use.

APPENDIX 5 - PSN ACCEPTABLE USAGE POLICY AND PERSONAL COMMITMENT STATEMENT

1. Introduction

PSN stands for Public Service network. This is a secure wide area network (WAN) that allows access to Central Government systems, secure data transfer, secure email and accredited solutions provided by public sector organisations and accredited 3rd parties. At present this includes gcsx secure email, CIS(Benefits), TellUsOnce and Electoral Registration systems. The scope of the PSN network covers local authorities, central government departments, National Health Service, the Criminal Justice Extranet and the Police National Network. Some Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd users will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include users having access to a secure email facility. All users requiring access to the PSN network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement.

This policy and statement does not replace the councils or Rykneld Homes existing acceptable usage, or any other, policies. It is a supplement to them.

2. Scope

All users of the PSN connection must be aware of the commitments and security measures surrounding the use of this network. This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers using the GCSx facilities.

3. Principles

It is Bolsover District Council, North East Derbyshire District Council and Rykneld Homes policy that all users of PSN understand and comply with corporate commitments and information security measures associated with PSN.

4. PSN Acceptable Usage Policy

Access control rules and procedures are required to regulate who can access Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing North East District Council, Bolsover District Council and Rykneld Homes Ltd. information in any format, and on any device.

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

4.1 Policy statement

Each PSN user must read, understand and sign to verify they have read and accepted this policy.

- I understand and agree to comply with the security rules of my organisation.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

i. I acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes.

ii. I agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,

iii. I will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse; and,

iv. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,

v. I will not attempt to access any computer system that I have not been given explicit permission to access; and,

vi. I will not attempt to access the PSN other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,

vii. I will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry; and,

viii. I will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,

ix. I will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received); and,

x. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material; and,

xi. I will appropriately label, using the HMG Security Policy Framework (SPF), information up to RESTRICTED sent via the PSN; and,

xii. I will not send PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information over public networks such as the Internet; and,

xiii. I will always check that the recipients of e-mail messages are correct so that potentially sensitive or PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information is not accidentally released into the public domain; and,

xiv. I will not auto-forward email from my GCSx account to any other non-GCSx email account; and,

xv. I will not forward or disclose any sensitive or PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and,

xvi. I will seek to prevent inadvertent disclosure of sensitive, PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information by avoiding being overlooked when working, by taking care when printing information received via PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted; and,

xvii. I will securely store or destroy any printed material; and,

xviii. I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via PSN (this will be in accordance with the Computer, Telephone and Desk Use Policy - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation); and,

xix. where IT Services has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,

xx. I will make myself familiar with the Councils or Rykneld Homes security policies, procedures and any special instructions that relate to PSN; and,

xxi. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security Information Security Incident Management Policy; and,

xxii. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,

xxiii. I will not remove equipment or information from council premises without appropriate approval; and,

xxiv. I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with the Council's Remote Working Policy; and,

xxv. I will not introduce viruses, Trojan horses or other malware into the system or PSN; and,

xxvi. I will not disable anti-virus protection provided at my computer; and,

xxvii. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant (please refer to the Legal Responsibilities Policy); and,

xxviii. if I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's email and records management policy.

Document Date:	[Date signed and agreed by user]
Name of User:	[Surname, First Name]
Position:	[Position]

Department:	[Department]
User Access Request Approved by:	[Line Manager Name – Position] [Date]
User Access Request Approved by:	[IT Services Asset Owner(s)] [Date]
Username Allocated	[Username]
Email Address Allocated:	[Email Address]
User Access Request Processed:	[IT Services] [Date]

4.2 PSN Personal Commitment Statement

I, [insert User's Name], accept that I have been granted the access rights to GCSx. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this policy, personal commitment statement, and the authorities Information Security policies. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Councils or Rykneld Homes's disciplinary policy, whichever is appropriate.

Signature of User: …….

A copy of this agreement is to be retained by the User and Information Security Manager.

APPENDIX 6 - HUMAN RESOURCES INFORMATION SECURITY STANDARDS POLICY

1. Introduction

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. hold large amounts of personal and protectively marked information. Information security is very important to help protect the interests and confidentiality of the councils, Rykneld Homes and their customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

Details of the National Protective Marking Scheme and Government Security Classifications can be found in the PSN acceptable usage policy and the ICT Policy Summary.

2. Scope

This policy applies to all users that require access to the councils or Rykneld Homes information systems or information of any type or format (paper or electronic).

The definition of users within this policy is intended to include all Departments, partners, employees of North East Derbyshire District Council, Bolsover District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to ICT equipment

Where access is to be granted to any third party (e.g. contractors, service providers, voluntary agencies, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with the councils or Rykneld Homes user that initiates this third party access.

3. Principles

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to the councils or Rykneld Homes information systems **must**:

- Be suitable for their roles.
- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any users access to information or information systems used to deliver the councils and Rykneld Homes business.

Access to the councils and Rykneld Homes information systems will not be permitted until the requirements of this policy have been met.

4. Roles and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the Information Asset Owner – please refer to Information Protection Policy (see Appendix 7).

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the ICT Section in a timely manner, using an agreed process.

The information security responsibilities of every user include familiarisation with the Information Security Policy and its Appendices, and the signing of a statement confirming that the user is aware of, and understands, these policies. (See Appendix 13)

4.1 User Screening

Background verification checks are carried out on all employees by HR, please see the HR recruitment and selection policy for details.

From January 2014 all users who require access to services or data delivered by the Public Services Network (PSN), including gcsx email **must** be cleared to "Baseline Personnel Security Standard".

From January 2015 all users who access the computer network of Bolsover District Council, North East Derbyshire District Council or Rykneld Home Ltd **must** be cleared to "Baseline Personnel Security Standard".

Where access is to systems processing payment card data, credit checks on the user must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

All the requirements for verification checks are applied to technical support and temporary users that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets).

4.2 Management Responsibilities

Line managers must notify ICT in a timely manner of any changes in a users role or business environment, to ensure that the user access can be changed as appropriate.

Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to a users access must be made in a timely manner and be clearly communicated to the user.

Departmental managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate Councils and Rykneld Homes policies. These policies include:

- Information Protection Policy (Appendix 7)
- Information Security Incident Management Policy (Appendix 11)

This requirement must be documented.

4.3 Information Security Awareness, Education and Training

All users will receive appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role.

It is the role of Departmental managers to ensure that their users are adequately trained and equipped to carry out their role efficiently and securely.

5. Applying the Policy – When Access to Information or Information Systems is No Longer Required

5.1 Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. information assets is removed in a timely manner when no longer required by the user

5.2 Return of Assets

Users must return all of the organisation's assets, for example, laptops, mobile phones, memory sticks in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

APPENDIX 7 - INFORMATION PROTECTION POLICY

1. Introduction

Information is a major asset that Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the councils and Rykneld Homes maintains. It also covers the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. The policy specifies the means of information handling and transfer within the councils and Rykneld Homes.

2. Scope

The policy applies automatically to all the systems, people and business processes that make up the councils and Rykneld Homes information systems.

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to Information systems or information used for the councils or Rykneld Homes purposes.

3. Principles

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. will ensure the protection of all information assets within the custody of the councils and Rykneld Homes.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

This policy should be applied whenever the councils or Rykneld Homes Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.

- Stored tape, DVD or video.
- Speech.

4. Applying the Policy

4.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

The councils and Rykneld Homes must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

4.2 Classifying Information

At present Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd have not implemented corporate document classification. However users may come into contact with documents classified under the Government classification schemes and must understand these and apply as appropriate when using Government ICT systems and gcsx email.

In relation to Central Government ICT systems all information assets must be classified and labelled in accordance with the HMG Security Policy Framework (SPF). The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should

clearly indicate the classification. Information up to RESTRICTED and OFFICIAL(subject to descriptor)sent via GCSx must be labelled appropriately using the SPF guidance.

The SPF requires information assets to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependant on this scheme.

From April 2014 the classifications are:

- OFFICAL
- SECRET
- TOP SECRET

The classifications pre April 2014 may remain in circulation and are:

- Unclassified.
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.
- TOP SECRET.

4.3 Personal data

Personal data is any information about any living, identifiable individual. This could be customer, employee, or member personal data. The councils and Rykneld Homes is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998. Details of specific requirements can be found in the Legal Responsibilities Policy.

4.4 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

4.5 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

4.6 Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by users. All users must be informed of their responsibility for the documents they create.

4.7 Corporate Information Assets

For information assets whose use throughout the councils or Rykneld Homes is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

4.8 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Users are not allowed to access information until a line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

Databases holding personal information have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information.

Files which are identified as a potential security risk should only be stored on secure network areas.

5. Disclosure of Information

5.1 Sharing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) Information with other Organisations

PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

Disclosing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) or OFFICIAL(subject to descriptor) information to any external organisation is also **prohibited**, unless via the Government Connect Secure Extranet (GCSx) email. Emails sent between Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. addresses are held within the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT, RESTRICTED and OFFICIAL(subject to descriptor) material. For further information see Email Policy.

An official email legal disclaimer must be contained with any email sent. This can be found in the Email Policy.

The disclosure of PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information in any way other than via GCSx email is a disciplinary offence. If there is suspicion of a user treating PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information in a way that could be harmful to the council or Rykneld Homes or to the data subject, then it is be reported to the internal audit section, and the person may be subject to disciplinary procedure.

Any sharing or transfer of the councils or Rykneld Homes information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

APPENDIX 8 - COMPUTER, TELEPHONE AND DESK USE POLICY

1. Introduction

Modern day business operations and advances in technology have necessitated the wide spread use of computer facilities into most offices within North East Derbyshire District Council, Bolsover District Council and Rykneld Homes Ltd. and, with the advent of portable computers, away from the councils and Rykneld Homes premises.

As such, there is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for the pursuance of personal interests or for amusement/entertainment. The councils and Rykneld Homes also handle large amounts of PROTECT, RESTRICTED and OFFICIAL information. The security of this information is of paramount importance. Working towards a clear desk policy can help prevent the security of this information from being breached.

The purpose of this document is to establish guidelines as to what constitutes "computer and telephony resources", what is considered to be "misuse" and how users should work towards a clear desk environment.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to information systems or information used for Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. purposes.

3. Principles

This policy should be applied whenever users who access information systems or information utilise Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. computer and telephony resources.

Computer and telephony resources include, but are not restricted to, the following:

- Mainframe computers.
- Departmental computers.
- Personal computers.
- Portable laptop computers.
- Terminals.
- Printers.
- Network equipment.
- Telecommunications facilities.

4. Computer Resources Misuse

No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case will need to be taken into account. However, some examples are outlined below:

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- Storing/loading/executing of software for a purpose which is not work related.
- Storing/loading/executing of software:
    - which has not been acquired through approved council or Rykneld Homes procurement procedures, or
    - for which the councils or Rykneld Homes does not hold a valid program licence, or
    - which has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose which is not work related.

For further information, users are requested particularly to read the following policies:

- Email Policy (Appendix 1)
- Internet Acceptable Use Policy (Appendix 2)
- Software Policy (Appendix 3)

.

5. Clear Desk

North East Derbyshire District Council, Bolsover District Council and Rykneld Homes Ltd. would wish to ensure that all information is held securely at all times. Ideally, work should not be left on desks unattended and should be removed from view when unsupervised.

At the end of each day, wherever possible, desks should be cleared of all documents that contain any marked under the Government Security Classification schemes, these include classifications of PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) or any information relating to staff, clients or customers. This information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level. If employees find this difficult because of accommodation issues, the matter should be raised with their Line Manager in the first instance.

Unclassified material, together with non North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd and specific operating manuals may be left tidily on desks. A definition of the Government marking schemes can be found in the ICT Policy Summary Document.

Documents should not be left lying on printers, photocopiers or fax machines.

Users of IT facilities are responsible for safeguarding data by ensuring that equipment is not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Computer screens must be locked to prevent unauthorised access when unattended and screens should lock automatically after a 10 minute period of inactivity, in order to protect information. A screen saver with password protection enabled must be used on all PCs. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action. The screen saver should be the one supplied by IT, no personal screen savers are to be used.

Users of hot desk stations must ensure that it is left in the state in which it was found.

Remember, when you are not working at your workstation there could be a business requirement for other users to use that station.

6. Legislation

Users should understand the relevant legislation relating to Information Security and Data Protection, and should be aware of their responsibilities under this legislation. The following statutory legislation governs aspects of the councils and Rykneld Homes information security arrangements. This list is not exhaustive:

- The Freedom of Information Act 2000.
- The Human Rights Act 1998.
- The Electronic Communications Act 2000.
- The Regulation of Investigatory Powers Act 2000.
- The Data Protection Act 1998.
- The Copyright Designs and Patents Act 1988.
- The Computer Misuse Act 1990.
- The Environmental Information Regulations 2004.
- The Re-use of Public Sector Information Regulations 2005.

Individuals can be held personally and legally responsible for breaching the provisions of the above Acts. Familiarisation with, and adherence to, the policies within this document will protect employees from breach of the provisions of the legislation mentioned above.

APPENDIX 9 - REMOTE WORKING

1. Introduction

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. provide portable computing devices to assist users to conduct official councils or Rykneld Homes business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of North East Derbyshire District Council, Bolsover District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who use Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd IT facilities and equipment when working on official business away from the organisation (ie working remotely), or who require remote access to Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd information Systems or information.

3. Principles

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. information systems or information must not be accessed whilst outside the United Kingdom regardless of who owns the IT equipment.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Smartphones
- Tablets
- Tablet PCs.
- PDAs.
- Palm pilots.
- Mobile phones.
- Text pagers.
- Wireless technologies.

4. Applying the Policy

All IT equipment (including portable computer devices) purchased for users by one of the Councils or Rykneld Homes is the property of the purchaser. It must be returned upon

the request of the purchaser. Access for ICT Services users of North East Derbyshire District Council or partners shall be given to allow essential maintenance security work or removal, upon request.

All IT equipment will be supplied and installed by North East Derbyshire District Council ICT Service staff. Hardware and software **must only** be provided by the purchasers.

Where users access Central Government IT systems including secure email, **under no circumstances** should non-Council owned equipment be used.

Definition of the national protective marking scheme can be found in the PSN acceptable usage policy (see appendix 5).

5. User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users will not install or update any software on to a council or Rykneld Homes owned portable computer device.
- Users will not install any screen savers on to a council or Rykneld Homes owned portable computer device.
- Users will not change the configuration of any council or Rykneld Homes owned portable computer device.
- Users will not install any hardware to or inside any councils or Rykneld Homes owned portable computer device, unless authorised by North East Derbyshire District Council ICT department.
- Users will allow the installation and maintenance of Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd installed Anti Virus updates immediately.
- Users will inform the ICT Section of any council or Rykneld Homes owned portable computer device message relating to configuration changes.
- Business data should be stored on a councils or Rykneld Homes file and print server wherever possible and not held permanently on the portable computer device
- All faults must be reported to the ICT Section.
- Users must not remove or deface any asset registration number.
- Users registration must be requested from the ICT Section. Users must state which applications they require access to.
- Users requests for upgrades of hardware or software must be approved by a line manager. Equipment and software will then be purchased and installed by ICT Services.
- The IT equipment can be used for personal use by users so long as it is not used in relation to an external business and does not conflict with Council business or policies. Only software supplied and approved by Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. can be used (e.g. Word, Excel, Adobe, etc.).

- No family members may use the ICT equipment. The ICT equipment is supplied for the users sole use.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. may recover the costs of repair.
- The user must not take any council or Rykneld Homes supplied ICT equipment outside the United Kingdom as the equipment may not be covered by the councils or Rykneld Homes normal insurance against loss or theft and it is liable to be confiscated by airport security personnel.
- Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database, or carry out any processing of PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information relating to the councils, Rykneld Homes, its employees, or customers. **Under no circumstances** should personal or security marked information be emailed to a private non-council or Rykneld Homes email address. For further information, please refer to the Email Policy.
- Any data transferred from Council systems must only be undertaken using a Council provided encrypted memory stick.
- Any member of users accessing PSN type services or facilities, or using PSN PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information, must only use councils or Rykneld Homes owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely.
- Users should not leave computer devices in unattended vehicles.
- Any loss of equipment should be reported immediately to the ICT Service Desk and, if appropriate, to the Data Protection Officer.

6. Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use

Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. No removable media devices or paper documentation should be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people, and the onus is on the employee to maintain confidentiality. Documents should be

collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information must be shredded.

7. Access Controls

It is essential that access to all PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or user login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) data held on the portable device must be encrypted. Personal data can only be stored on encrypted devices. It is ICTs responsibility to provide encrypted devices and the employees to ensure they are used.

An SSL or IPSec VPN must be configured to allow remote users access to the councils or Rykneld Homes systems if connecting over Public Networks, such as the Internet. If connecting to PSN resources, this **must** be an IPSec-VPN.

Dual-factor authentication must be used when accessing the council network and information systems (including Outlook Web Access) remotely via both the council or Rykneld Homes owned and non-council owned equipment

Access to the Internet from Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. owned ICT equipment, should only be allowed via onward connection to the councils or Rykneld Homes provided proxy servers and not directly to the Internet. It is the employees responsibility to ensure this.

8. Anti Virus Protection

Users who work remotely must ensure that the anti Virus software is kept up-to-date on their portable computer devices by either connecting to the corporate network or the Internet (depending on how the device is configured) at least once every two weeks to enable the anti virus software to be updated.

9. Users Awareness

All users must comply with appropriate codes and policies associated with the use of IT equipment as contained within the Information Security Policy and its appendices.

It is the user's responsibility to ensure their awareness of and compliance with these.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. are.

APPENDIX 10 - REMOVABLE MEDIA POLICY

1. Introduction

This policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd. computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

A definition of the national protective marking scheme and government security classifications can be found in the PSN acceptable usage policy (see appendix 5).

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to North East Derbyshire District Council, Bolsover District Council or Rykneld Homes Ltd. information systems or IT equipment and intends to store any information on removable media devices.

3. Principles

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official councils or Rykneld Homes business.

Removable media devices include, but are not restricted to the following

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines)
- Video tapes

4. Risks

Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. recognises that there are risks associated with users accessing and handling information in order to conduct official council or Rykneld Homes business. Information is used throughout the councils and Rykneld Homes and sometimes shared with external organisations and applicants. Securing PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) data is of paramount importance – particularly in relation to the council's need to protect data in line with the requirements of the Data Protection Act 1998 Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the councils or Rykneld Homes. It is therefore essential for the continued operation of the councils and Rykneld Homes that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the councils and Rykneld Homes needs.

5. Restricted Access to Removable Media

It is Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. policy to prohibit the use of all removable media devices without approval. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the IT Section. Approval for their use must be given by the ICT Manager, this should be done via a request to the service desk. This applies to the devices themselves, including memory sticks but not the media such as CD's, DVD's and audio and video tapes.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

6. Procurement of Removable Media

All removable media devices, including memory sticks, and any associated equipment and software must only be purchased and installed by ICT Services. Procurement of consumable media such as CD's, DVD's and audio and visual may be procured through standard procurement channels. Non-council owned removable media devices and media **must not** be used to store any information used to conduct official council or Rykneld Homes business, and **must not** be used with any council or Rykneld Homes owned or leased IT equipment.

The only equipment and media that should be used to connect to councils or Rykneld Homes equipment or the councils or Rykneld Homes network is equipment and media that has been purchased by the councils or Rykneld Homes and approved by the ICT Section or has been sanctioned for use by the IT Manager.

7. Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for the councils or Rykneld Homes purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system. For further information please see the Remote Working Policy (see Appendix 9).

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) data or personal or sensitive data held must be encrypted.

Users should be aware that the councils and Rykneld Homes will audit / log the transfer of data files to and from all removable media devices and council or Rykneld Homes owned IT equipment.

8. Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the ICT Section who will access the breach to determine the

appropriate course of action. The Data Protection Officer should also be informed where appropriate.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the ICT Manager as referenced in the Information Security Incident Management Policy (see Appendix 11).

9. Third Party Access to Council or Rykneld Homes Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the councils or Rykneld Homes network, information stores or IT equipment without explicit agreement from the ICT Manager.

Should third parties be allowed access to the councils or Rykneld Homes information then all the considerations of this policy apply to their storing and transferring of the data.

10. Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the ICT Section should removable media be damaged and return to ICT for secure disposal.

Virus and malware checking software approved by the ICT Section must be operational on any device managed and owned by the Council. It is the users responsibility to ensure appropriate and up to date virus and malware software is operational on any non Council device that the removable media device is connected to or seek assurances to that effect.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the councils or Rykneld Homes, other organisations or individuals from the data being lost whilst in transit or storage.

11. Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the councils or Rykneld Homes or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. **All removable media devices that are no longer required, or have become damaged, must be returned to ICT Services for secure disposal**.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the ICT Section.

12. Users Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices.

APPENDIX 11 - INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

1. Introduction

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An information security incident includes, but is not restricted to, the following (see paragraph *** below for more detailed examples):

- The loss or theft or corruption of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Bolsover District Council, North East Derbyshire District Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. information systems or IT equipment.

All users **must** understand and adopt use of this policy and are responsible for ensuring the safety and security of the councils or Rykneld Homes systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.

- Receiving unsolicited mail of an offensive nature.

- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Sending a sensitive e-mail to 'all staff' by mistake
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. computer equipment.

4. Procedure for Incident handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the ICT section in order to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the ICT section to gain as much information as possible from the business users to identify if an incident is occurring.

The following sections detail how users must report information security events or weaknesses.

4.1 Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from ICT support staff.
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the ICT Service Desk on ext 3001 or external number 01246 217103.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported immediately to senior management and the Data Protection Officer for the impact to be assessed.

The ICT Section will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

The Data Protection Officer will require:

- A contact name and number of the person reporting the incident
- Type of data
- Details of steps already taken

4.2 Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to ICT Services. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by ICT Services.

4.3 Collection of Evidence

If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact the ICT Section for advice.

The actions required to recover from the security incident must be under formal control. Only identified and authorised users should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

The officer responsible for an incident should risk assess the incident based on the Risk Impact Matrix

4.4 Risk Impact Matrix

To decide on the potential or actual impact of an information security incident, the impact matrix below should be used.

Type of Impact	Reputational Media and Member Damages	Reputational Loss within Government and / or Failure to Meet Statutory / Regulatory Obligations	Contractual Loss	Failure to meet Legal Obligations	Financial Loss / Commercial Confidentiality Loss	Disruption to Activities	Personal Privacy Infringement
Low	None	None	None	None	None	None	None
	Contained internally within the council or Rykneld Homes Unfavorable council member response	Internal investigation or disciplinary involving one individual	Minor contractual problems / minimal SLA failures	Civil lawsuit / small fine - less than £10K	Less than £100,000	Minor disruption to service activities that can be recovered	Personal details revealed or compromised within department
Medium	Unfavorable local media	Government authorised investigation by	Significant client dissatisfaction. Major SLA	Less than £100K Damages	£100,000 - £500,000	Disruption to service that can be recovered	Personal details revealed or compromised

	interest Unfavorable council member response	nationally recognised body or disciplinary involving 2 to 9 people	failures. Failure to attract new business	and fine		with an intermediate level of difficulty. One back up not backing up for 2 or more days	internally within authority. Harm mental or physical to one member of staff or public
High	Sustained local media coverage, extending to national media coverage in the short term	Government intervention leading to significant business change. Internal disciplinary involving 10 or more people	Failure to retain contract(s) at the point of renewal	Greater than £100K damages and fine	£500,000 - £1,000,000	Major disruption to service which is very difficult to recover from. Two or more systems not being backed up for two or more days	Severe embarrassment to individual(s)

	Sustained unfavorable national media coverage	Service or product outsourced through Government intervention	Client contract(s) cancelled	Over £1M damages and / or fine Custodial sentence(s) imposed	More than £1,000,000	Catastrophic disruption - service activities can no longer be continued	Detrimental effect on personal & professional life OR large scale compromise affecting many people. Harm mental or physical to two or more members of staff or public

APPENDIX 12 - IT INFRASTRUCTURE SECURITY POLICY

1. Introduction

The purpose of this policy is to establish standards in regard to the physical and environmental security of the councils and Rykneld Homes information, in line with section A9 of ISO/IEC/27001.

In order to ensure the continued protection of the personal, confidential and protectively marked information(see Glossary) information that Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. holds and uses, and to comply with legislative requirements, information security best practice, and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Public Services Network(PSN), access to Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd. information equipment and information must be protected.

Definition of the national protective marking scheme can be found in the PSN acceptable usage policy (appendix 5).

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the councils and Rykneld Homes IT data centre. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. No service should fall below the baseline security standard level of protection required for their teams and locations.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all departments, partners, employees of Bolsover District Council, North East Derbyshire District Council and Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. information equipment and information (electronic and paper records). They are responsible for ensuring the safety and security of the councils and Rykneld Homes equipment and the information that they use or manipulate.

3. Principles

There shall be no unauthorised access to either physical or electronic information within the custody of the councils or Rykneld Homes.

Protection shall be afforded to:

- Records containing sensitive data/personal information.
- IT equipment used to access electronic data.
- IT equipment used to access the councils and Rykneld Homes network.

This policy applies to all users of the councils or Rykneld Homes owned or leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to the councils and Rykneld Homes should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution users make to the safe and secure use of information within the custody of the councils and Rykneld Homes.

This policy should be applied whenever a user accesses the councils or Rykneld Homes information or information equipment. This policy applies to all locations where information within the custody of the councils or Rykneld Homes or information processing equipment is stored, including remote sites.

4. Secure Areas

PROTECT, RESTRICTED and OFFICIAL(subject to descriptor)information **must** be stored securely. A risk assessment should identify the **appropriate** level of protection to be implemented to secure the information being stored.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.

- Protection against damage - e.g. fire, flood, vandalism.

Access to secure areas such as the data centre and ICT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Users working in secure areas should challenge anyone not wearing a staff or visitor badge. Each department must ensure that doors and windows are properly secured at the end of each working day.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A council ICT employee must monitor all visitors accessing secure ICT areas at all times.

Keys to all secure areas housing ICT equipment and lockable ICT cabinets are held centrally by the ICT department, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach.

If a user leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the users and any door/access codes should be changed immediately. Please also refer to the ICT Access Policy and Human Resources Information Security Standards.

5. Non-Electronic Information Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification as stated in Information Protection Policy. If it is classified as PROTECT, RESTRICTED or OFFICIAL(subject to descriptor), information security controls to protect it must be put in place. A risk assessment should identify the appropriate level of protection for the information being stored. Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet.
- Locked safes.

- Stored in a Secure Area protected by access controls.

6. Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from ICT Services.

All items of equipment must be recorded on an inventory, both on the departmental and the information services inventory. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the departmental and the ICT inventories.

For portable computer devices please refer to the Remote Working Policy (appendix 9).

7. Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be

protected by conduit and where possible avoid routes through public areas, Health and Safety guidance should be sought if in any doubt.

8. Security of Equipment off Premises

The use of equipment off-site must be formally approved by the user's line manager. Equipment taken away from Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted if carrying PROTECT, RESTRICTED or OFFICIAL(subject to descriptor) information.
- Be password protected.
- Be adequately insured.

Further information can be found in the Removable Media Policy (appendix 10) and Remote Working Policy (appendix 9).

Users should ensure, where necessary and required, that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the ICT Department who will inform Internal Audit, the Finance Section and the Data Protection Officer.

Users should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act.

9. Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must be returned to ICT for data removal.

Software media or services must be returned to ICT to be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

APPENDIX 13 - ICT INDUCTION DECLARATION

ICT INDUCTION DECLARATION

NAME: _____

DEPARTMENT: _____

COURSE TITLE: ICT Induction

DATE OF ATTENDANCE: _____

I confirm that I have attended the above course and have been fully advised in respect of the Council's policies governing usage of the ICT facilities including the Internet and E-mail systems.

I undertake to comply with all ICT Policies during my period of employment with the Council/Rykneld Homes Ltd*. (* delete as applicable)

Signed (inductee) ----------

Dated ----------

Signed (ICT) ----------

Appendix 2

Members' ICT Charter

The following are points which Members are asked to take into account to make the Council's ICT and smart-phone support streamlined and efficient. It also helps to ensure that the IT equipment provided is fit for purpose.

1. Contact and support – All ICT issues should be raised by contacting **Martin Derbyshire, Members IT and Training Officer, on 7010** in the first instance and otherwise **Service Desk** on **3001 (Internal)** , **01246 217103 (External)** or by **email** at servicedesk@ne-derbyshire.gov.uk. (Please note members have responsibility for their own broadband arrangements where they have declined Council provided broadband).

2. All new members should undergo induction before receiving their laptop, iPad or smart-phone so they are aware of the policies and procedures that are pertinent to IT usage at the Council.

3. Specific guidance and advice is available for the use of iPads and members should familiarise themselves with this. It is available via the Members' Portal.

4. For the convenience of members, the Council has developed a structured plan of annual health checks for laptops, iPads and smart-phones. All members are requested to agree to this plan which will help keep laptops and iPads in good condition and minimise problems. Your schedule for health checks will be issued so you can see when these have been arranged. If any of the dates in your plan are inconvenient please contact the Members' IT and Training Officer to schedule a mutually convenient time.

5. Members should not install any third party software. Extra software other than standard build items should have a business requirement. This is because installation of untested software can impact on the performance of the laptop or iPad and could possibly introduce viruses on to the Council's systems. Please contact the Governance Team if you wish to install additional software on your laptop, iPad and smart-phone.

6. Laptops, iPads and smart-phones issued to members by the Council are to be used only by the members themselves. They should not be shared, transferred, loaned or used for access by anyone other than the designated member.

7. Whilst members may use laptops, iPads and smart-phones for non work web browsing, they must avoid viewing, creating, circulating, distributing, storing, downloading or printing material that might be considered offensive, illegal, pornographic or sexually explicit, that brings the Council into disrepute or that exposes it to legal action. Members should also be careful not to use Council resources for party political purposes.

8. Storage of a limited amount of personal information on the laptop, iPad and smart-phone is permitted but this is not recommended because it can affect the performance of the device and any information lost cannot be recovered.

9. Members should note that information held by a member on their electronic device is subject to the terms of the Data Protection Act 1998 and the Freedom of Information Act 2000 and therefore such devices are included within the scope of any relevant requests or internal reviews made under the terms of these Acts.

10. It is not considered appropriate for officers to be asked by members to transfer personal information between devices or to provide support for non-Council related activities.

11. The Council can take no responsibility for any information lost on a laptop, iPad or smart-phone. The loss of any equipment should be reported to the Members' IT and Training Officer and to the Data Protection Officer as soon as possible so that a breach log can be filed and an assessment made as to the risk of such a loss.

12. Members should apply the housekeeping techniques demonstrated at their induction to ensure that their mailbox is available at all times. Advice and guidance on these techniques will be given at the induction. The Members' IT and Training Officer is always available for advice and guidance.

13. Security awareness sessions will be provided by the Governance Team to ensure members can work safely and securely with Council provided ICT services and equipment. Members must make all reasonable endeavours to attend this training.

14. Members should endeavour to attend any user training sessions provided by the Governance Team or Joint ICT Service to help maintain and update their ICT knowledge and skills. These will be flexible and arranged around member needs.

15. Members who are no longer office holders should return their laptop, I-Pad, smart phones and other Council provided equipment as soon as possible, but no later than 10 working days from leaving office.

.

16. Members should endeavour to keep within the 2 GB monthly connection limit when using their iPads. Usage can be monitored via the My Data Usage App.

By adhering to the above conditions it will help the Council to facilitate its paperless working concept that has been adopted.

Cabinet Office

Government Security Classifications

April 2014

Version 1.0 – October 2013

THE GOVERNMENT SECURITY CLASSIFICATIONS WILL COME INTO FORCE ON 2 APRIL 2014

Version History

SPF Version	Document Version	Date Published	Summary Of Changes
N/A	1.0	Dec 12	Document created.
N/A	1.0	Apr 13	Annex - Security Controls Framework added.
11.0	1.0	Oct 13	N/A – This document will replace the current 'Government Protective Marking Scheme' document on 2 April 2014.

Government Security Classifications

Executive Summary

This policy describes how HM Government classifies information assets to: ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

Everyone who works with government has a duty to respect the confidentiality and integrity of any HMG information and data that they access, and is personally accountable for safeguarding assets in line with this policy.

HMG information assets may be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.

Government Departments and Agencies should apply this policy and ensure that consistent controls are implemented throughout their public sector delivery partners (i.e. NDPBs and Arms Length Bodies) and wider supply chain.

The Government Security Classifications will come into force on 2 April 2014 - until then existing policy remains extant.

Cabinet Office
October 2013

Government Security Classifications

Overview of Key Principles

1. This policy describes HM Government's administrative system for the secure, timely and efficient sharing of information. It is not a statutory scheme but operates within the framework of domestic law, including the requirements of the Official Secrets Acts (1911 and 1989), the Freedom of Information Act (2000) and the Data Protection Act (1998).

> **Principle One:**
> **ALL** information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

2. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification:

OFFICIAL	SECRET	TOP SECRET
The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.	HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

3. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. A top level controls framework is provided as an annex to this policy. As a minimum, all HMG information must be handled with care to comply with legal and regulatory obligations and reduce the risk of loss or inappropriate access. There is no requirement to mark routine OFFICIAL information.

4. Organisations may need to apply controls above (or below) the baseline on a risk managed basis appropriate to local circumstances and in line with HMG risk appetite tolerances. The Government SIRO will moderate such instances that entail any pan-government risk.

5. The classification scheme applies to information (or other specific assets). Major ICT infrastructure (e.g. large aggregated data sets, payments systems, etc.) may require

enhanced controls to effectively manage associated confidentiality, integrity and availability risks – determined on a case by case basis following a robust risk assessment.

Principle Two:
EVERYONE who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

6. Accidental or deliberate compromise, loss or misuse of HMG information may lead to damage and can constitute a criminal offence. Individuals are personally responsible for protecting any HMG information or other assets in their care, and must be provided with guidance about security requirements and how legislation relates to their role, including the potential sanctions (criminal or disciplinary) that may result from inappropriate behaviours. A summary of the relevant legal and regulatory context is set out on page 13.

7. Organisations must have a breach management system in place to aid the detection and reporting of inappropriate behaviours, enable disciplinary procedures to be enforced and assist with any criminal proceedings.

Principle Three:
Access to **sensitive** information must **ONLY** be granted on the basis of a genuine 'need to know' and an appropriate personnel security control.

8. Information needs to be trusted and available to the right people at the right time. The failure to share and exploit information can impede effective government business and can have severe consequences (e.g. medical records or case management files). The principles of openness, transparency, Open Data and information reuse require individuals to consider the proactive publishing of public sector information and data sets. However, this must always be a reasoned judgement, taking data protection and confidentiality into account.

9. The compromise, loss or misuse of sensitive information may have a significant impact on an individual, an organisation, or on government business more generally. Access to sensitive information must be no wider than necessary for the efficient conduct of an organisation's business and limited to those with a business need and the appropriate personnel security control. This 'need to know' principle applies wherever sensitive information is collected, stored, processed or shared within government and when dealing with external public and private sector organisations, and international partners.

10. The more sensitive the material, the more important it is to fully understand (and ensure compliance with) the relevant security requirements. In extremis, there may be a need to share sensitive material to those without the necessary personnel security control, for example when immediate action is required to protect life or to stop a serious crime. In such circumstances a **common sense** approach should be adopted - if time permits, alternatives should be considered and steps taken to protect the source of information. If there is any doubt about providing access to sensitive assets, individuals should consult

their managers or security staff before doing so and when time permits record the reasons for their actions.

Principle Four:
Assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

11. The policy applies equally to assets entrusted to HMG by others, such as foreign governments, international organisations, NGOs and private individuals.

12. Where specific reciprocal security agreements / arrangements are in place with foreign governments or international organisations, equivalent protections and markings must be recognised and any information received must be handled with AT LEAST the same degree of protection as if it were UK information of equivalent classification. Detailed information about international and bilateral security agreements and the controls for managing foreign-originated information is set out in the 'International Protective Security Policy' supplement to the SPF.

13. Where no relevant security agreements / arrangements are in place, information or other assets received from a foreign country, international organisation or a UK NGO must at a minimum be protected to an equivalent standard as that afforded to HMG OFFICIAL assets, although higher classifications may be appropriate. Refer to the 'International Protective Security Policy' supplement for more detail.

14. The need to know principle must be strictly enforced for access to international partners' information.

Security Classification Definitions

15. The three security classifications (OFFICIAL, SECRET and TOP SECRET) indicate the increasing sensitivity of information AND the baseline personnel, physical and information security controls necessary to defend against a broad profile of applicable threats:

- The typical threat profile for the **OFFICIAL** classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.
- The threat profile for **SECRET** anticipates the need to defend against a higher level of capability than would be typical for the OFFICIAL level. This includes sophisticated, well resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors. Reasonable steps will be taken to protect information and services from compromise by these actors, including from targeted and bespoke attacks.
- The threat profile for **TOP SECRET** reflects the highest level of capability deployed against the nation's most sensitive information and services. It is assumed that advanced state actors will prioritise compromising this category of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated.

OFFICIAL

Definition:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level.

This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile described in paragraph 15 above, and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

Baseline Security Outcomes:

- **ALL** HMG information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice (described in the Annex).

Marking:

There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes.

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

16. Data Owners are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate.

17. To support specific business requirements and compartmentalise information, organisations may apply an optional DESCRIPTOR, alongside the OFFICIAL-SENSITIVE classification marking, to distinguish particular types of information and indicate the need for additional common sense precautions to limit access. Further detail is provided in paragraph 21 below.

SECRET

Definition:

Very sensitive HMG (or partner's) information that requires protection against the highly capable threat profile described in paragraph 15, **AND** where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Directly threaten an individual's life, liberty or safety (from highly capable threat actors).

b. Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:

   i. Current or future capability would be rendered unusable;

ii. Lives would be lost; or,

iii. Damage would be caused to installations rendering them unusable.

c. Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.

d. Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.

e. Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.

f. Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.

g. Cause major impairment to the ability to investigate or prosecute serious organised crime.

Baseline Security Outcomes:

- Make accidental compromise or damage highly unlikely during storage, handling, use, processing, transmission, transport or disposal.
- Offer an appropriate level of resistance to deliberate compromise by forced and surreptitious attack.
- Where possible, detect actual or attempted compromise and help to identify those responsible.

Marking:

All information in this security domain should be clearly and conspicuously marked **'SECRET'**. Information that requires more restrictive handling due to the nature or source of its content may merit a special handling instruction; see paragraphs 18 – 26 below.

TOP SECRET

Definition:

Exceptionally sensitive HMG (or partner's) information assets that directly support (or threaten) the national security of the UK or allies **AND** require extremely high assurance of protection from all threats (as set out in paragraph 15). This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Lead directly to widespread loss of life.

b. Threaten directly the internal stability of the UK or friendly nations.

c. Raise international tension.

d. Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks.

e. Cause exceptionally grave damage to relations with friendly nations.

f. Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

g. Cause long term damage to the UK economy.

h. Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.

Baseline Security Outcomes:

- Prevent accidental or deliberate compromise or damage during storage, handling, use, processing, transmission, transport or disposal.
- Offer robust resistance against compromise by a sustained and sophisticated or violent attack.
- Detect actual or attempted compromise and make it likely that those responsible will be identified.

Very little information risk to such data and services can be tolerated unless there is full and explicit understanding by the SIRO in line with HMG risk appetite tolerances.

Marking:

All such information should be clearly and conspicuously marked **'TOP SECRET'.** Information that requires more restrictive handling due to the nature or source of its content may merit a special handling instruction; see paragraphs 18 – 26 below.

Special Handling Instructions

18. Security classifications are the principle means of indicating the sensitivity of a particular asset and the requirements for its protection. Special handling instructions are additional markings which can be used in conjunction with a classification marking to indicate the nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures.

19. Special handling instructions should be used sparingly and only where the sensitivity justifies strict restrictions on information sharing. Individuals must be given guidance on how to mark and work with assets bearing special handling instructions.

20. A supplementary control framework for handling material derived from intelligence is provided in the SPF.

DESCRIPTORS

21. Organisations may apply a DESCRIPTOR to identify certain categories of **sensitive** information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes. Descriptors should be used in conjunction with a security classification and applied in the format: '**OFFICIAL-SENSITIVE [DESCRIPTOR]'**

22. Cabinet Office maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments:

    - **'COMMERCIAL':** Commercial- or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed.
    - **'LOCSEN':** Sensitive information that locally engaged staff overseas cannot access.
    - **'PERSONAL':** Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals, or the personal / medical records of people in sensitive posts (e.g. military, SIA).

23. Descriptors must not be applied to information that is sent to overseas partners (unless formally agreed in advance) as they are not recognised under any international agreements and are likely to cause confusion.

CODEWORDS

24. Codewords provide security cover for a particular asset or event. A Codeword is a single word expressed in CAPITAL letters and is placed immediately after the classification marking. They are usually only applied to SECRET and TOP SECRET assets. Codewords are co-ordinated centrally by the Defence Crisis Management Centre and must be allocated by the centre's Operational Support team.

PREFIXES AND NATIONAL CAVEATS

25. Specific markings may be used either to indicate the provenance of sensitive information, or as a means to control dissemination.

    a. UK Prefix - ALL assets sent to foreign governments or international organisations, must be marked with a UK prefix, both to designate the originator and to inform any decision about possible disclosure under existing or future Freedom of Information (FOI) legislation in the country concerned. SECRET and TOP SECRET assets should include the following instruction:

    b. National Caveats may be used to designate assets of particular sensitivity to the UK or where dissemination must be restricted to individuals from specific foreign nations. Unless explicitly named, information bearing a national caveat must not be sent to foreign governments, overseas contractors, international organisations or released to any foreign nationals (either overseas or in the UK) without the originator's consent. Information should be marked in the format 'CLASSIFICATION – CAVEAT', e.g:

'TOP SECRET – UK / US EYES ONLY'

With the exception of British Embassies and Diplomatic Missions or Service units or establishments, assets bearing the UK EYES ONLY national caveat must only be sent overseas in exceptional circumstances and where access by British nationals can be strictly controlled.

Time Sensitive Information

26. In carefully controlled circumstances, it may be appropriate for some high-value, high-threat information to be managed at a lower classification to capitalise on immediate business and/or operational benefits, for example where the value of the information is time limited and short term. Such 'one off' exceptions must be carefully considered and the organisation's Senior Information Risk Owner (SIRO) must fully understand the longer term risk implications for their business given that an adversary may invest to discover vulnerabilities now that can be very quickly capitalised on in the future. This is particularly important if the same capabilities are used frequently or over an extended period to protect many instances of short term value information.

Working with Security Classifications

27. Security classifications can be applied to any asset that has value to the business. This includes information in whatever form (but not the IT systems used to store or process classified information), items of equipment, hardware and other valuables. Classification markings should be clear and conspicuous, including any special handling instructions. Where it is impractical to apply a marking (e.g. on equipment), staff must be made aware of the protection and procedures required. Where an asset has inherent transferable value or the nature of the item dictates the need for special handling (e.g. firearms, toxic / atomic materials etc.), organisations must ensure that appropriate (in some cases, statutory) controls are in place to protect against compromise, loss or damage.

28. When working with information assets, the following points need to be considered:

- There is no requirement to explicitly mark routine OFFICIAL assets.
- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise.
- When working with documents, classifications must be in CAPITALS at the top and bottom of each page. More sensitive information should be separated into appendices, so the main body can be distributed widely with fewer restrictions.
- Sensitive material published on intranet sites must also be clearly marked.
- It is good practice to reference the classification in the subject line and / or text of email communications. Where practicable systems should compel users to select a classification before sending, e.g. via a drop-down menu.
- Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Every effort should be made to consult the originating organisation before a sensitive asset is considered for disclosure, including release under FOIA or to the National Archives.
- A file, or group of sensitive documents or assets, must carry the highest marking contained within it. For example, a paper file or an e-mail string containing OFFICIAL and SECRET material must be covered by the higher marking (i.e. SECRET).
- E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an e-mail 'string' before they add to it and forward it on.
- In certain circumstances there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitised digest or pre-agreed form of words at a lower classification in anticipation of such a requirement.
- Where practicable, time-expiry limits should be considered so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g. official statistics.

Valuing technology assets: Confidentiality, Integrity and Availability

29. ICT systems need to keep information confidential, but also maintain the integrity and availability of information and / or services. The degree of impact on the business from a loss of availability or integrity may vary and should be considered as part of a comprehensive risk assessment process that takes into account threat, vulnerability, likelihood and mitigations. 'HMG IA Standard Numbers 1 and 2 – Information Risk Management' describes the process of assessing and managing risk to ICT systems.

30. In certain contexts (e.g. nuclear or air safety), the loss or compromise of integrity or availability may be so catastrophic that enhanced controls to mitigate these risks will be required even if the likelihood seems slight. Moreover, there are statutory security requirements that must be upheld in number of specialist fields, such as atomic materials, air safety, firearms, and witness protection.

31. The compromise of a significant volume of data (e.g. personal data) is likely to have a higher impact than the loss of individual information assets, and may merit more restrictive handling controls. Likewise, the inter-connectivity of different data sets may allow more sensitive connections to be made by association. **Aggregation, accumulation and association** of data (within ICT systems and on removable media) must be carefully considered as part of the risk management process as additional protective controls may or may not be appropriate.

Physical Security: Risk Assessment Methodologies

32. Physical security controls for the protection of HMG assets should be applied according to layering principles. A risk assessment is required to determine applicable threats and risks.

33. Once the threat(s) to the information is/are understood, and prior to purchasing or deploying a new security system or product, an Operational Requirement (OR - a structured methodology for determining security requirements) should be undertaken. Best practice guidance is available in the CPNI 'Guide to Operational Requirements for Security Measures'.

34. Where assets require protection from surreptitious attack, the 'Security Assessment for Protectively Marked Assets' (SAPMA) risk assessment methodology should be completed to determine suitable additional security controls to prevent or detect compromise.

Legal Framework

The UK classification system operates within the framework of domestic law. This includes:

a. **Official Secrets Act 1989:** Damage assessment is a critical element of the OSA, most of the offences in which require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or special investigation powers, or of confidential information received from a foreign State or an international organisation. With respect to each type of information, the OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it. Different offences apply to: members of the security and intelligence services; persons notified under section 1 of the OSA; Crown servants; government contractors; and any person.

b. **Data Protection Act 1998**: The handling of personal data must be in compliance with the DPA. The DPA, however, contains a number of exemptions to some or all of the data protection principles and to other provisions of the DPA such as the right of access to personal data. For example, section 28 provides an exemption from the data protection principles and a number of other provisions of the DPA if it is required for the purpose of national security. But note that, although the exemption is widely drawn, it is only available to the extent that it is required for the purpose of national security. Thus departments and agencies will still be required to assess whether it is possible to address national security concerns and comply with the DPA. Other exemptions, such as section 29 (crime and taxation) are more narrowly drawn. Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one applies. Departments and agencies should also have regard to the DPA, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

c. **Freedom of Information Act 2000:** Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

d. **Public Records Act 1967.** Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

Annex - Security Controls Framework

Version 1.0 – April 2013

Summary

This Annex to the Government Security Classifications policy (December 2012) describes the physical, personnel and information security controls required to provide a proportionate and robust level of protection for assets at each of the three classification levels (OFFICIAL, SECRET and TOP SECRET).

Within each level, assets must be protected to broadly consistent standards wherever they are collected, stored, processed or shared across HM government and with wider public sector and external partners. This consistency is essential to provide the confidence that underpins effective information sharing and interoperability between organisations.

The Annex is provided in three sections:

- **Part One – Threat Model and Security Outcomes:** providing the context and objectives underpinning risk management decisions.
- **Part Two – Working with HMG Assets:** typical security controls that individuals should apply when working with information (and other assets) at each classification.
- **Part Three – Protecting Assets and Infrastructure:** high level principles to help organisations determine appropriate security requirements for the protection of ICT infrastructure / services, and other assets.

This document should be read in conjunction with the detailed standards and guidance set out in the HMG Security Policy Framework (SPF).

Cabinet Office
April 2013

Part One - Threat Model and Security Outcomes

1. Security classifications indicate the sensitivity of information AND the typical controls necessary to defend HMG assets against a broad profile of applicable threats. Risk owners should appreciate that information classified at one level cannot be assured to be protected against the threat profile associated with a higher level of classification.

OFFICIAL

2. The OFFICIAL tier provides for the generality of government business, public service delivery and commercial activity. This includes a diverse range of information, of varying sensitivities, and with differing consequences resulting from compromise or loss. OFFICIAL information must be secured against a threat model that is broadly similar to that faced by a large UK private company. This anticipates defending data and services against compromise by attackers with bounded capabilities and resources, including (but not limited to): hactivists, single-issue political pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

3. This model does not imply that information within the OFFICAL tier will not be targeted by some sophisticated and determined threat actors (including Foreign Intelligence Services) who may deploy advanced capabilities. It may be. Rather, a risk based decision has been taken not to invest in controls to assure protection against those threats, i.e. proportionate not guaranteed protection.

4. Technical controls at this level will be based on assured, commercially available products and services, without need for any bespoke development. Whilst these controls cannot absolutely assure against the most sophisticated and determined threat actors, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access OFFICIAL information.

SECRET

5. The SECRET threat model anticipates a higher level of threat capability than would be typical for the threat model described in the OFFICIAL tier. The model includes threat sources such as elements of serious and organised crime as well as some state actors. Attacks may be bespoke in nature and tailored to specifically attack the target infrastructure. Vulnerable elements of the supply chain may be targeted to facilitate a further compromise of information. The opportunities for accidental compromise of information will be minimised, with technical protection where possible.

6. Risk owners should appreciate that assured protection will not be provided against very sophisticated, persistent and blended attacks by the most capable and determined organisations (such as highly competent state actors). A level of risk acceptance is required, that these threat sources have the capability to successfully target information within this tier if they are motivated to do so.

TOP SECRET

7. The TOP SECRET threat model reflects the highest level of capability deployed against the nation's most sensitive information and services. Very little risk can be tolerated in this tier, although risk owners should note that no activity is entirely free from any risk.

Security Outcomes

To defend against these typical threat profiles, protective security controls should achieve the following outcomes at each classification level:

	OFFICIAL	SECRET	TOP SECRET
Outcome	• Meet legal and regulatory requirements • Promote responsible sharing and discretion • Proportionate controls appropriate to an asset's sensitivity • Make accidental compromise or damage unlikely	• Make accidental compromise or damage highly unlikely • Detect and resist deliberate attempts at compromise • Make it highly likely those responsible will be identified	• Prevent unauthorised access • Detect actual or attempted compromise • Identify those responsible and respond appropriately
Personnel Security	• Access by authorised individuals for legitimate business reasons	• Assurance that access is only by known and trusted individuals	• High assurance that access is strictly limited to known and trusted individuals
Physical Security (handling, use, storage, transport and disposal)	• Proportionate good practice precautions against accidental or opportunistic compromise • Control access to sensitive assets through local business processes and dispose of with care to make reconstitution unlikely	• Detect and resist deliberate compromise by forced and surreptitious attack • Destroy / sanitise to make reconstitution and / or identification of constituent parts highly unlikely	• Robust measures to prevent compromise by a sustained and sophisticated or violent attack • Destroy / sanitise to prevent retrieval and reconstitution
Information Security (storage, use, processing or transmission)	• Protect against deliberate compromise by automated or opportunist attack • Aim to detect actual or attempted compromise and respond.	• Detect and resist deliberate compromise by a sophisticated, determined and well resourced threat actors	• Robust measures to prevent compromise from sustained attack by sophisticated, determined and well resourced threat actors

Part Two: Working with HMG Assets

8. This section describes typical personnel, physical and information security controls required when working with HMG assets. The indicative controls table should be used as the basis for local security instructions and processes.

9. The identified controls are cumulative - minimum measures for each classification provide the baseline for higher levels.

10. Organisations may need to apply controls above (or below) the baseline to manage specific risks to particular types of information. Such exceptions must be agreed with the respective data owners and delivery partners. The Government SIRO will moderate any instances that entail pan-government risk.

11. Security requirements must be set out in local security instructions and reinforced by training to ensure that individuals understand their responsibilities. Organisations should operate an appropriate security culture commensurate with their particular circumstances and risk appetite.

12. HMG assets need to be managed to meet the following basic principles. More stringent controls may be appropriate to manage more sensitive assets:

    a. Handle with care to avoid loss, damage or inappropriate access. Compliance with applicable legal, regulatory and international obligations is the minimum requirement.

    b. Share responsibly, for business purposes. Use appropriately assured channels as required (e.g. internal HMG email) and provide meaningful guidance on specific sensitivities and handling requirements.

    c. Store assets securely when not in use. For example, implement clear desk policies and screens locking when ICT is left unattended.

    d. Where assets are taken outside the office environment they should be protected in transit, not left unattended and stored securely. Precautions should be taken to prevent overlooking or inadvertent access when working remotely or in public places.

    e. When discussing HMG business in public or by telephone, appropriate discretion should be exercised. Details of sensitive material should be kept to a minimum.

    f. Particular care should be taken when sharing information with external partners or the public; for example, emails, faxes and letters should only be sent to named recipients at known addresses.

    g. Information that is not freely available in the public domain should be destroyed in a way that makes reconstitution unlikely. More sensitive assets should be returned to the office for secure disposal where appropriate.

    h. Report any incidents involving theft, loss or inappropriate access to HMG assets.

13. The below table describes standard control measures when working with information assets at each classification level. It should be read in conjunction with the detailed policy and guidance set out in the Security Policy Framework (SPF).

14. At OFFICIAL, the controls are recommended as good practice for all routine information, but organisations may want to adopt a more directive approach to control access to particularly sensitive information (e.g. information handled with the OFFICIAL-SENSITIVE caveat).

	OFFICIAL	SECRET	TOP SECRET
Personnel Security (Refer to the SPF Personnel Security paper for detailed guidance)	Minimum controls include: • Appropriate recruitment checks (e.g. the BPSS, or equivalent) • Reinforce personal responsibility and duty of care through training • 'Need to know' for sensitive assets	Additional minimum controls include: • Always enforce Need to Know • SC for regular, uncontrolled access • Special Handling Instructions	Additional minimum controls include: • DV for regular, uncontrolled access
Physical Security c. Document handling	• Clear desk / screen policy • Consider proportionate measures to control and monitor access to more sensitive assets	• Register and file documents in line with locally determined procedures • Maintain appropriate audit trails • Control use of photocopiers and multi-function digital devices in order to deter unauthorised copying or electronic transmission • Limit knowledge of planned movements to those with a need to know	• Register movement of documents and undertake annual musters • Conduct random spot checks of documents to ensure appropriate processing / handling / record keeping and record results • Strictly limit knowledge of planned movements to those with a need to know
d. Storage	• Storage under single barrier and / or lock and key • Consider use of appropriate	• Defence in Depth • Use of CPNI Approved Security Furniture (refer to CSE)	• Robust measures to control and monitor movements • Information must be accountable

	OFFICIAL	SECRET	TOP SECRET
	physical security equipment / furniture (see the CPNI 'Catalogue of Security Equipment', CSE)	• Segregation of shared cabinets • Proportionate measures to control and monitor access / movements	
e. Remote Working	• Ensure information cannot be inadvertently overlooked whilst being accessed remotely • Store more sensitive assets under lock and key at remote locations	• Risk assessment to determine need and identify appropriate protective security controls • CPNI approved security furniture at remote location (see CSE) • Approval may need to be sought from the originator	• Only to be removed for remote working as an exception if determined essential and following acceptance of the inherent risks by senior management
f. Moving assets by hand:	• Single cover • Precautions against overlooking when working in transit • Authorisation required for significant volume of records/files	• Risk Assess the need for two people to escort the movement of document(s)/media • Documented local management approval required and completion of document / media removal / movement register • Sealed tamper-evident container / secure transportation products (refer to CSE) • Not accessed in public areas	• Senior Manager approval subject to risk assessment
g. Moving assets by post / courier	• Include return address, never mark classification on envelope • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable	• Local Management approval required, actions recorded in document movement register • Robust double cover • Approved registered mail service commercial courier ('track and	• Senior Manager approval subject to risk assessment • Special handling arrangements may need to be considered

	OFFICIAL	SECRET	TOP SECRET
	commercial courier's 'track and trace' service	trace'), or Government courier	
h. Moving assets overseas (by hand or post)	• Trusted hand under single cover • Consider using reputable commercial courier's 'track and trace' service	• Trusted hand (appropriate security clearance, e.g. SC) • Sealed tamper evident container / secure transportation products (refer to CSE) • Where travelling to / via a country of 'Special Security Risk' the container should be carried by a diplomatically accredited courier	• Security cleared (DV) diplomatically accredited courier only
i. Bulk Transfers (Volume thresholds may vary by organisation and should be defined in local policies)	• Local management approval, subject to departmental policy, appropriate risk assessment and movement plans	• Senior management approval, subject to departmental policy, appropriate risk assessment and movement plans • Commercial companies could be used provided information transported in sealed containers/ crates, accompanied by departmental staff and movement and contingency plans are in place	• Local police aware of movement plan
INFORMATION SECURITY[1] a. Electronic Information at	• Electronic Information will be protected at rest by default. This may be appropriate physical protection (such as data at rest in a government data centre) or	• Electronic Information will normally be protected at rest by physical security appropriate for SECRET assets. Where data is at rest on non-physically secure devices it	• Electronic Information will normally be protected at rest by physical security appropriate for TOP SECRET assets. Where data is at rest on non-physically secure

[1] NB. Information Security Controls are described in greater detail in part three of this annex.

	OFFICIAL	SECRET	TOP SECRET
Rest	may involve Foundation Grade data at rest encryption when physical control isn't guaranteed (such as on a laptop)	will be encrypted with (revitalised) Enhanced Grade protection	devices it will be encrypted with High Grade protection
b. Electronic Information in Transit	• Information in transit between Government or other trusted organisations will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption • Information may be emailed / shared unprotected to external partners / citizens, subject to local business policies and procedures • Where more sensitive information must be shared with external partners (e.g. citizens), consider using secure mechanisms (e.g. browser sessions using SSL / TLS)	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) Enhanced Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems
c. ICT Services	• Different GCloud services will be suitable for different types of OFFICIAL information. Risk owners MUST read and understand any GCloud accreditation residual risk statements	• ICT Services must be accredited as appropriate considering the SECRET threat model. CESG design patterns or bespoke advice may be required • Very careful risk assessment and understanding of implications of	• ICT systems designed must be accredited as appropriate considering the TOP SECRET threat model. Bespoke architectural advice may be necessary

	OFFICIAL	SECRET	TOP SECRET
	• ICT services developed by a Department or delivery partner must follow the risk management processes as set out in HMG IA Standards IS1 and 2 and follow standard architectural approaches • End user devices will conform to the security principles defined in the *End User Device (EUD) Strategy: Security Framework and Controls*	enabling functionality • Information exchange outside of the SECRET tier will be highly constrained and managed using shared accredited capability	
d. Removable Media (data bearing)	• The use of removable media will be minimised, and other approved information exchange mechanisms should be used where available in preference • Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement • Consider appropriate encryption to protect the content, particularly where it is outside the organisation's physical control	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection
Telephony (mobile	• Details of sensitive material	• Secure Telephony, VTC and	• Secure Telephony, VTC and

	OFFICIAL	SECRET	TOP SECRET
and landline), Video Conference and Fax	should be kept to a minimum • Recipients should be waiting to receive faxes containing personal data and / or data marked with the OFFICIAL – SENSITIVE caveat	secure fax	secure fax

Disclosure
(Statutory disclosures are separate from the classification scheme and require case-by-case assessment)
	• Much of the information in this domain is likely to be releasable unless an FOI exemption is in force, it is personal data subject to the Data Protection Act, or there is another statutory bar
	• Official Secrets Act (OSA) and criminal cases subject to damage tests.
	• Where appropriate, non-sensitive information should be published for reuse
		• Likely to engage FOIA exemption in whole or in part (e.g. 23, 24, 26, 27, 31), to be assessed on a case by case basis
		• Some information might be releasable in a securely redacted format
			• Subject to a case by case assessment there is a general presumption that information is:
			  • above the OSA Prosecution threshold
			  • subject to FOIA exemptions on National Security (or other) grounds

Archiving and Transfer to The National Archives	• Transfer as open records wherever possible, at 20 years and in accordance with the Public Records Act	• Retain as long as classification level applies	• Retain as long as classification level applies
Disposal / Destruction	• Dispose of with care using approved commercial disposal products to make reconstitution unlikely (refer to CPNI guidance and HMG IS5.)	• Verify document is complete before destruction • Use approved equipment and or service providers listed in the CSE	• Control measures to witness / record destruction

	OFFICIAL	SECRET	TOP SECRET
	• Guidance about the physical destruction of assets is available in 'CPNI Requirements for Secure Destruction', March 2013. • Electronic media used to process HMG assets must be sanitised and disposed of in accordance with the requirements in 'HMG IA Policy No. 5 - Secure Sanitisation.'		
Incident Reporting	• Local reporting arrangements • Escalation to DSO and SIRO as appropriate for significant incidents • ICO notified of "significant" losses of personal data • GovCert / CINRAS for ICT incidents	• DSO and SIRO notified, local procedures followed • Consider notifying Accounting Officer and responsible Minister • ICO notified if personal information • May be appropriate for Police investigation subject to damage test and Cabinet Office gateway process	• Accounting Officer, Minister and Cabinet Office alerted
	• Guidance about the management and handling of security incidents is available in the SPF documents 'Security Breach Management' and 'Leaks Procedural Guidance'. Relevant ICO guidance should also be consulted.		

Part Three – Protecting Assets and Infrastructure

15. This section is intended to help security practitioners and information risk professionals to determine appropriate security requirements for the protection of infrastructure, ICT systems / services, and other assets at each level of the classification system.

16. It outlines context, process and security considerations at a high level but cannot, of itself, provide the level of detail necessary to implement specific technical architectures or deploy a new security system or product. It must be read in conjunction with the detailed policy, guidance and structured risk assessment methodologies set out in the Security Policy Framework.

Physical Security Principles:

17. Physical security controls should be applied appropriately, mindful of the 'layering principles'. A risk assessment is required to determine the applicable threats and risks.

18. Once the threats to an asset are understood, and prior to purchasing or deploying a new security system, an 'Operational Requirement' (OR) should be completed to determine an appropriate blend of physical security controls (and counter-terrorism controls where applicable). The Catalogue of Security Equipment (CSE) lists suitable products, graded 'Base', 'Enhanced' or 'High' to reflect performance in resisting forced attack.

19. Where assets require protection against surreptitious attack (i.e. espionage), a 'Security Assessment of Protectively Marked Assets' (SAPMA) should be completed to determine whether additional security controls may be required. Appropriate products are detailed in the CSE, rated as CPNI Classes 1 to 4 to reflect the different levels of skill / knowledge of the attacker and the resources available to them.

20. Where it is not feasible to protect the entirety of a large or bulky item (e.g. tanks, aircraft, ammunition etc), the most sensitive elements of the item should be protected using appropriate CSE products. Enhanced procedural controls may also be appropriate, for example, additional vetting and / or guarding.

Information Security Principles

21. Information at any level of classification should receive broadly consistent levels of protection across the Public Sector. This consistency is essential to establish trust between organisations and promote greater interoperability.

22. The broad risk appetite for information types will be overseen by the appropriate pan-government governance body. For the OFFICIAL and SECRET tiers this will be the Senior Cyber and Risk Assurance Board (SCaRAB) and the Office of the Government SIRO (OGSIRO). For the TOP SECRET tier this will be the Information Sharing Policy Board (ISPB) and the SIA Release Authorities.

23. Public Sector organisations continue to own and manage their own information risk, within the bounds of the top level HMG risk appetite set by the SCaRAB / ISPB. Within this framework there remains an enduring requirement for organisations to assess their own information risks and make appropriate accreditation decisions which balance risk with realising business opportunities.

24. Departmental SIROs are responsible for managing Departmental risk with SCaRAB / ISPB responsible for shared or pan-Government risk. The OGSIRO should be consulted if local decisions exceed the HMG risk appetite (as set out in the *HMG Information Risk Directive*) AND there is a pan-government impact.

25. ALL Public Sector ICT systems must be appropriately accredited, although accreditation activities should be proportionate to the system functionality and level of information risk. Where shared services have existing or a community accreditation (e.g. the Public Services Network (PSN) and G-Cloud services), then Departments can rely on this assurance providing it supports their own risk appetite (including understanding of any documented residual risks). This supports the ICT Strategy Programmes "accredit once, use many" model.

Confidentiality, Integrity and Availability Considerations

26. The Classification Policy relates to Confidentiality requirements. However, Public Sector information and services often have significant Integrity and/or Availability requirements too. There exist many scenarios where the consequences of a loss of Integrity or Availability can be significantly more severe than a loss of Confidentiality.

27. A high Integrity or Availability requirement does not lead to a high classification. A holistic risk assessment must be conducted, which includes the consideration of risks to Confidentiality, Integrity and Availability respectively. Treatment of significant Integrity or Availability requirements may require robust technical controls and a high level of assurance, over and above that indicated by the (Confidentiality driven) classification.

Sensitive Information

28. Some particularly sensitive information will attract a Caveat (e.g. OFFICIAL-SENSITIVE) or Special Handling Instructions (e.g. CODEWORDS or National Caveats) to denote the need for further controls, particularly in respect of sharing. The impact of compromise of this information may be higher, but this does not imply that it will necessarily be subject to the threat model applicable to higher tiers.

29. Such information can be managed at the same classification level, but with a more prescriptive information handling model, potentially supported by extra procedural or technical controls to reinforce the need to know. The aim of additional technical controls is to manage the information characteristics that attract the additional marking (for example enforcing access control, or technically limiting the number of records a user can view). These controls will be data and system dependent.

Aggregation

30. As government employs greater sharing and reuse of commoditised ICT solutions as well as shifting public services delivery to online channels, there is potential for large volumes of data objects to be concentrated in a small number of systems or services, or for a single system to provide a large number of government services.

31. Aggregation of data or services may result in the following conditions being realised:

- The impact to the business from the loss, compromise or misuse of an aggregated data set is likely to be higher than the impact of compromise of a single object. The increase in impact can, under some circumstances, be severe (such as very large sets of citizen data);
- Existing Threat Sources will remain relevant but these threats may be more motivated to mount an attack as the benefit to them of compromising a large number of data objects is more appealing;
- Threat Sources may be attracted to attack the aggregated data set or service because the return on investment may be sufficiently increased. This is especially relevant when considering aggregation of value bearing transactions. These Threat Sources may therefore deem it worthwhile to deploy an increased technical capability.

32. Aggregated data sets should be considered to be within the same classification level; however where the impact of compromise or loss has increased as a result of aggregation, these aggregated data sets must be carefully and tightly controlled.

33. Aggregation of data at rest on end user devices, or the aggregated presentation of data to end user devices must be avoided as far the business requirement allows. This minimises the impact of compromise of the device or of inappropriate action from the user (accidental or malicious). This may include technical controls to physically limit the data or services being accessed, as well as transactional monitoring approaches to detect and respond to anomalous data or service access.

34. A risk assessment must be undertaken to determine the specific technical controls needed to protect the aggregated data set – this will include an understanding of how aggregation affects threat. Technical controls to protect an aggregated data set should be robust and risk owners may decide that they require a higher level of assurance or additional technical capability (such as fault tolerance). The risk assessment for the given aggregated service or data set should determine the specific technical controls within an appropriate architecture.

Assessing the impact on the Business [2]

[2] N.B. Work is underway to refocus business impact assessment as a qualitative process that forms part of the overall risk assessment. A transition plan for introducing the new process, terminology and rule set will be available by October 2013; this section will be updated in due course.

35. Organisations are required to assess the potential impact to the business in the event that specific information risks are realised. This assessment should form part of a comprehensive risk assessment which also considers threat, vulnerability and likelihood. This risk assessment process considers Confidentiality, Integrity and Availability of information independently.

36. Within each tier there will be a range of information with varying degrees of business impact should the risks be realised – this is particularly true when considering the OFFICIAL tier.

37. The existing Business Impact Level (BIL) structure should continue to be used in the course of an information risk assessment process. BIL's should not on their own be used to 'label' information systems or indicate a level of accreditation. In due course the BIL policy will be revised to provide a qualitative assessment process that supports the genuine business priorities. There is no direct mapping between existing BILs and any given classification.

Security Enforcing Functionality

38. Where any security functionality or security product is relied upon, there must be confidence that those products or functions are effective and are providing the protection that is expected of them. All such products must therefore have an appropriate level of independent validation or assurance, proportionate to the classification of the information they are used to protect.

Information Assurance Policy and Guidance

39. Information Assurance Standards and good practice guidance set out in the HMG Security Policy Framework (SPF), as well as additional products in CESG's IA Policy Portfolio, remain extant. Many of these documents describe good practice which is agnostic of classification labels.

40. Documents that specifically reference the former Government Protective Marking System (GPMS) and/or BILs will over time be updated or withdrawn. In the interim period 'transition' guidance will be available to help organisations use the existing good practice advice with the new Classification Policy.

Technical Controls Summary

OFFICIAL

41. ALL HMG information assets have value and require an appropriate level of protection, whether in transit, at rest or whilst being processed. Pan-government interoperability and trusted sharing are founded on mutual assurance that organisations apply consistent risk management approaches and that information will receive broadly equivalent levels of protection. At OFFICIAL, a de facto common baseline of protection is provided through a framework of controls:

    - Any legal obligations (e.g. DPA) or regulatory requirements;
    - The broad risk appetite for OFFICIAL, set out in the *HMG Information Risk Directive;*
    - SPF policy and guidance, including this Control Framework, HMG Information Assurance Standards and CESG's good practice guidance;
    - Common assurance and accreditation processes, including the Baseline Control Set (BCS);
    - Common security compliance regimes (e.g. GSI / PSN Codes of Connection);
    - UK Government Reference Architecture;
    - Common trusted infrastructure offerings delivered through the ICT Strategy programmes (End User Devices, Public Services Network, G-Cloud and G-hosting), noting that any residual risks should be managed in line with local risk appetites;
    - HMG ICT Moratorium and Spend Controls Processes.

42. There is a diverse range of government business and information at OFFICIAL. Within this broad framework, there is an onus on risk owners to understand the business value and sensitivity of their information and the ways in which they work with and share it. This will determine specific Confidentiality, Availability and Integrity requirements that manage the precise risks to any particular asset within the OFFICIAL baseline.

43. OFFICIAL information will normally be protected utilising appropriately assured, commercially available security products and service offerings. Government will not seek to create bespoke products or ICT services to manage information risk at this level.

44. Where assurance of security enforcing functionality is required, products should be certified against the relevant Security Characteristics for that class of product. Assurance will normally be delivered through industry led (but independent) assessments under the CESG Commercial Product Assurance (CPA) scheme (Foundation Grade), though other assurance processes may be appropriate following a suitably scoped risk assessment or validation exercise.

45. Whilst Foundation Grade security product assurance or service offerings will be industry led, some CESG oversight may be appropriate where these products or services are being provisioned to, for example, a sufficiently sized proportion of the Public Sector as to present a 'national level' of risk.

46. OFFICIAL information will be accessed and shared using a variety of methods, including the internet, GSi and PSN. Information in transit should be protected by default, unless there are sensible business reasons where this is not appropriate and the business can tolerate the risk. In practice, use of encryption would be expected to secure (for example) the following information exchanges:

    - OFFICIAL data at rest on End User Devices and removable media;
    - Remote access connections and sessions (e.g. VPN) into secure environments such as a corporate network or cloud service;
    - Transactional services (e.g. payment services) delivered to the citizen over untrusted networks;
    - Connections between networks or interconnections within a geographically separated network – i.e. at the infrastructure (not user) level, between Public Sector organisations[3];
    - Information that relates to or directly supports National Security.

47. There is no policy requirement to encrypt routine (email) information exchanges with external partners (citizen, industry, local government, third sector). However, where sensitive information (or routine personal data) is exchanged over untrusted infrastructure with external partners, consideration should be given to protecting it using technologies such as client-side email encryption, or providing access to information via a secure browser session, (such as an individual using SSL/TLS to view online banking information or webmail).

48. Service offerings supporting the OFFICIAL tier will be commercially based. These services could be delivered by industry (with industry led independent assessment), or developed as a Public Sector service but still utilising commercial technologies. Organisations will have to make risk informed decisions as to what type of service is appropriate based on their business requirements. For example, the business requirement to host a public information service will necessitate the use of a different type of service offering, from a requirement to process personal medical data. Security enforcing products within the service offering would be expected to be independently validated or assured as described above.

49. Public Sector organisations will increasingly be expected to utilise shared services delivered through pan-government ICT programmes. These programmes will provide a range of commoditised products and service offerings, with different security characteristics and levels of assurance. Organisations that plan to utilise these shared services and infrastructure to manage assets at OFFICIAL must read the detailed technical standards and guidance developed for the relevant programme, along with any statements of residual risk associated with the use of a particular product or service:

    Public Services Network (PSN)

3 NB. Encryption is increasingly becoming standard commercial practice to protect information in transit. It is anticipated that the availability of standard, easy to deploy and use encryption technology will lead to a future standard encrypted PSN, where encryption does not attract a cost premium. This single, protected environment will in future make secure interoperability straightforward and intuitive for the Public Sector.

50. The ICT Strategy anticipates that the PSN will be the primary network bearer for OFFICIAL information. PSN consuming organisations must comply with the *PSN IA Conditions*, and manage any stated residual risks inline with local risk appetites.

End User Devices (EUD)

51. The EUD programme anticipates that any OFFICIAL information (including information handled with the OFFICIAL-SENSITIVE caveat) can be managed on a single device that conforms to the security principles defined in the *End User Device Strategy: Security Framework and Controls*, (March 2013). Note that the assurance required (including compliance with relevant legislation such as Freedom of Information Act (FoIA) and DPA), means that EUDs will normally be owned, managed and controlled by the organisation. Any stated residual risks must be managed in line with local risk appetites.

G-Cloud

52. The G-Cloud programme anticipates that most OFFICIAL information can be managed through accredited service offerings available via the CloudStore. Service offerings will be accredited according to *G-Cloud Information Assurance Requirements and Guidance,* and any stated residual risks should be managed in line with local risk appetites. Three types of service are defined, that will likely be appropriate for different types of information and business processes:

    - Unassured Cloud services. These services (formerly Impact Level 00x) may be appropriate for a limited amount of information where there is no Confidentiality requirement (such as marketing and communications data intended for public consumption), although risk owners should consider whether they have Integrity or Availability requirements that must be managed.
    - Assured Public Cloud (formerly Impact Level 22x) services will be subject to a suitably scoped ISO27001 certification and other assurance activities as described in the *GCloud Information Assurance Requirements and Guidance.* Such services may be appropriate for the generality of OFFICIAL information, although organisations should carefully consider the scope of the IS027001 certification, the geographic location of the hosting, and any other residual risks identified as part of the G-Cloud Accreditation Statement. It is unlikely that these services will be suitable for more sensitive information.
    - Formally accredited Public Cloud (formerly Impact Level 33x) or Private Cloud services will be subject to a full HMG accreditation and will be hosted within the UK. These services are likely to be appropriate for most OFFICIAL information, although organisations should still be mindful of any risks involved in outsourcing services and data to the cloud (including those set out in the G-Cloud Accreditation Statement).

53. Organisations that are considering utilising G-cloud service offerings must note the following:

    - Off-shoring of information that relates to or supports National Security is prohibited.
    - The Office of the Government SIRO must review any plans to off-shore HMG data. Wherever possible, any personal data held off-shore should be kept within the EEA,

Safe Harbor or the limited number of countries with positive findings of adequacy from the European Commission.

Data Centre Consolidation:

54. The Data Centre Consolidation Programme (G-Hosting) anticipates reducing the number of Government (and public sector) data centres through a programme of virtualisation, consolidation and rationalisation. Security and resilience requirements for data centres will be determined on a site specific basis, aligned to broader initiatives to ensure appropriate protections for Critical National Infrastructure (CNI) assets.

SECRET

55. SECRET information must be very well protected against the defined threat model. The SECRET tier will be a largely isolated trust domain with only specific and assured information exchange functionality to less trusted domains.

56. SECRET ICT infrastructure will be physically or cryptographically isolated from less trusted domains (such as OFFICIAL ICT systems or the Internet). The only exceptions to this requirement will be:

- Gateways that provide specific business information exchange functionality. These gateways will require appropriate architectural assurance and as far as possible represent shared capability.
- At the discretion of SCaRAB where there is an overwhelming business requirement. Specific arrangements will be necessary to manage urgent operational imperatives.

57. Products protecting SECRET information will provide very robust protection that includes holistic security controls. The appropriate level of product assurance at SECRET is a revitalised and strengthened Enhanced Grade Standard; this will include a broader set of data separation technologies in addition to cryptography.[4]

58. The model for SECRET includes very sensitive information that is subject to a sophisticated threat, but much SECRET information doesn't carry an enduring long-term intelligence life. For some SECRET information that is very sensitive and is of enduring intelligence value, risk owners should carefully consider whether this information should in fact reside in the TOP SECRET tier.

TOP SECRET

59. High Grade assurance remains appropriate for TOP SECRET tier protection. This level of assurance will support UK sovereignty requirements.

[4] NB. More detailed information about the technical controls required for the protection of SECRET and TOP SECRET information will be set out in additional, classified guidance.

Publication date: October 2013

Any enquiries regarding this publication should be sent to us at GSSmailbox@cabinet-office.x.gsi.gov.uk

You can download this publication from www.gov.uk.

Appendix 4

Equality Impact Assessment

Responsibility and Ownership

Name of policy, practice, service or function: **IT Security Policy**

Responsible department: ……Joint IT Service…….

Service area: ……..

Lead Officer: Lee Thompson……...

Other members of assessment team

Name	Position	Area of expertise
Lee Thompson		
Liz Ball	Business Development Manager	
Lynne Cheong	Equality Improvement Officer	
Amar Bashir	Policy Officer	

Scope of the assessment

1	**What are the main aims/objectives or purpose of the policy, strategy, practice, service or function?**	To ensure continued delivery of services to organisations using the Joint IT Service To maintain public confidence through the highest standards of information security. To ensure compliance with relevant legislation for public bodies/providers of public services.
2	**Are there any external factors we need to consider like changes in legislation?**	N/A
3	**Who implements the policy, strategy, practice, service or function?**	Joint IT Service
4	**Who is affected by the policy, strategy, practice, service or function?**	Staff in all named organisations covered by the policies Residents & customers - vulnerability
5	**What outcomes do we want to achieve, why & for whom?**	Protected & secure data
6	**What existing evidence do you have on the impact of the policy, strategy, practice, service or function?**	
7	**How is information about the policy, practice, service or function publicised?**	Policies available to employees via publication on intranet. Relevant policies included in induction packs for all new employees.

Identifying Potential Equality Issues

Consider any impacts / barriers on each of the protected characteristics set out below and consider any that might cross over eg: between race / disability, gender / religion and belief, sexuality / age etc. Indicate where the policy, practice, service or function could have a positive or negative impact for different groups and your reasons. Specify which data sources have informed your assessment.

Race

8	**Identify any adverse impacts/barriers of the policy or procedure on people who may be disadvantaged because of their race**		
	White	English / Welsh / Scottish / Northern Irish / British	**N/A**
		Irish	
		Gypsy or Irish Traveller	
		Any other White background	
	Asian / Asian British	Indian	
		Pakistani	
		Bangladeshi	
		Chinese	
		Any other Asian background	
	Black / African / Caribbean / Black British	African	
		Caribbean	
		Any other Black / African / Caribbean / Black British background	
	Any other ethnicity	Arab	
		Any other ethnic group	

Sex / gender

9	Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of their gender	
	Female	N/A
	Male	
	Transgender	

Age

10	Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of their age	
	0-9 years	N/A
	10-15 years	
	16-18 years	
	19-24 years	
	25-34 years	
	35-44 years	
	45-54 years	
	55-59 years	
	60-64 years	
	65 years and over	

Disability		
11	**Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of their disability or long term ill health**	
	Physical or mobility impairments	N/A
	Sensory (hearing, visual, speech)	
	Mental health	
	Learning disabilities	
	Non-visible conditions such as epilepsy or diabetes	

Religion or belief		
12	**Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of their religion or belief, including non belief**	
	No religion	N/A
	Christian	
	Buddhist	
	Hindu	
	Jewish	
	Muslim	
	Sikh	
	Any other religion	

12	**Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of their religion or belief, including non belief**	
	Any other philosophical belief	

Sexual orientation

13	**Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of their sexual orientation**	
	Heterosexual	N/A
	Lesbian	
	Gay	
	Bisexual	
	Prefer not to say	

Other categories

13	**Identify any adverse impact/barriers of policy, practice, service or function on people who may be disadvantaged because of other factors**	
	Rural / urban	
	Carers	
	Child poverty	
	Social value	
	Any other	Remote working Access to secure data held with regard to vulnerable people; disabled customers; victims of crime; employees; frail & elderly residents. Reasonable adjustments for disabled staff are made via individual workplace assessment, so needs are met.

Analysing the information and setting equality objectives and targets

Service or function	Policy or practice	Findings	Which groups are affected and how	Whose needs are not being met and how?

Document the evidence of analysis

Data or information	When and how was it collected?	Where is it from?	What does it tell you?	Gaps in information
Customer feedback and complaints	IT user survey			
Consultation and community involvement				
Performance information including Best Value	Performance Information collected			
Take up and usage data	Potential to collect data on home working etc, as per IT Strategy.			
Comparative	Regional statistics	East Midlands Government Warning,		

Data or information	When and how was it collected?	Where is it from?	What does it tell you?	Gaps in information
information or data where no local information available	from local authorities on security breaches.	Advice and Reporting Point (EMGWARP) http://www.emcouncils.gov.uk/emgwarp-network		
Census, regional or national statistics	N/A			
Access audits or other disability assessments	HR individual workplace assessments for disabled employees.			
Workforce profile	Workforce data available for all participating organisations.			
Where service delivered under procurement arrangements – workforce profile	N/A			
Monitoring and scrutiny arrangements	Any security issues addressed as and when they arise by senior managers (Strategic Alliance Management Team, Joint Management			

Data or information	When and how was it collected?	Where is it from?	What does it tell you?	Gaps in information
	Board, Data Protection Officers).			

Recommendations and Decisions

Take immediate action by:

Amending the policy, strategy, practice, service or function	
Use an alternative policy, strategy, practice, service or function	
Develop equality objectives and targets for inclusion in the service plan	
Initiate further research	
Any other method (please state)	

All actions must be listed in the following Equality Impact Assessment Improvement Plan Summary

Equality Impact Assessment Improvement Plan Summary

Name of policy, practice, strategy, service or function …….

Department ……

Date of assessment …….

Please list all actions, recommendations and/or decisions you plan to take as a result of the equality impact assessment.

Recommendation/Decision	Action Required	Responsible Officer	Target Date	Resources	Progress	Actual Outcome

Please state where the departmental electronic assessment will be kept:

……

EIA Assessment Group

Date of assessment		
Sub group approval	Yes / No	
Subject to minor amendments	Yes / No	
Date published on corporate website		

Copies of all EIAs are stored on PERFORM.

The Council publishes its Equality Impact Assessments as evidence of the analysis that it undertook to establish whether its policies, strategies, practices, services and functions would further or would have furthered the 3 aims of the general equality duty, details of the information that it considered and details of engagement undertaken when doing the analysis.

The general duty requires the council to:

- Eliminate discrimination, harassment & victimisation
- Advance equality
- Foster good relations between different groups

Committee:	Union/Employee Consultation Committee	Agenda Item No.:	7.
Date:	12th March 2014	Category	*
Subject:	Pay Policy - Relief Central Control Operators.	Status	Open
Report by:	Joint Assistant Director of HR and Payroll		
Other Officers involved:	Housing Needs Officer (Relief Central Control Operators) Payroll Manager		
Director	Chief Executive Officer		
Relevant Portfolio Holder	Councillor E. Watts, Leader of the Council		

RELEVANT CORPORATE AIMS
STRATEGIC ORGANISATIONAL DEVELOPMENT – Continually improving our organisation by maintaining the Pay Agreement.
TARGETS
This report does not relate to any specific targets.
VALUE FOR MONEY
Having up to date policies will contribute to providing value for money services.

THE REPORT

The purpose of this report is to seek approval to make minor additions to the Pay Agreement to reflect current practice relating to the pay entitlement for employees carrying out central control duties on a relief basis.

At Council on 09 September 2009 Members approved the decision of UECC on 29 July 2009 to include the pay arrangements for Full time and Part time Central Control Operators in the Council's Pay Agreement.

For operational reasons, a number of employees now provide relief cover for this service. This has introduced a third category of Central Control Operators which the pay agreement does not cover. Pending formal agreement this new group of workers have been paid the appropriate rate of pay for Central Control operators with the accrual of annual leave in accordance with paragraph 3.2.10.

The 34% enhancement paid to part time central control operators does not apply to relief workers because reliefs are not required to work regular unsocial hours, regular shift working or provide regularly cover.

To reflect current practice, it is proposed that the following paragraph is added to paragraph 3.2.12 of the Council's Pay Policy:-

> "Relief Central Control Operators will receive Grade 7 for all hours worked and will accrue annual leave in accordance with paragraph 3.2.10 above."

Extracts from the existing pay agreement is attached at Appendix A for reference.

ISSUES FOR CONSIDERATION

The report section covers the issues for consideration.

Comments of the Director **(Delete from final version if no comments received)**.

IMPLICATIONS

Financial :	None as the report reflects current practice.
Legal :	None
Human Resources :	Clarifies the Pay Agreement to avoid incorrect payments.

RECOMMENDATION(S)

1. **That the following paragraph is added to paragraph 3.2.12 of the Council's Pay Agreement:-**
   "Relief Central Control Operators will receive Grade 7 for all hours worked and will accrue annual leave in accordance with paragraph 3.2.10 above."

ATTACHMENT: Y
FILE REFERENCE:
SOURCE DOCUMENT:

Appendix A

Extracts from the Pay Agreement paragraph are set out below.

3.2.10 **Enhancements in lieu of annual leave (amended)**

Casual workers are entitled to the equivalent of 28 days annual leave during each holiday year (including all bank holiday entitlements), calculated on a pro rata basis depending on the number of hours that actually worked.

Annual leave must be taken in line with the operational needs of the Council and agreed in advance with a supervisor. If any public holidays and/or 'fixed closure days' fall during the period of this engagement the casual worker may take annual leave on such days, with the agreement of their supervisor, from their accrued statutory leave entitlement.
When the arrangement for casual work is terminated the casual worker will be paid for holidays accrued but not taken on a pro rata basis.

Part time employees who work additional hours over and above their contractual hours may accrue additional annual leave on a pro rata basis based on the Council's annual leave entitlement and the additional hours.

3.2.12 **Central Control Operators**
This group of employees have unique features of their job as follows:-
• 24 hour three shift rota
• Working 8 hour shifts with no opportunity to leave the workplace
• Annual leave and sick leave subject to 'partner' covering shift
• Handover period at end of shift
• Exempt from Working Time Regulations based on need for continuity of service
• Exempt from taking strike action based on being a critical life and limb service
• Other organisations as customers
• Contractual requirements with Derbyshire County Council Supporting People

No other group of employees have all of these unique features.
With effect from 1st October 2009 these employees will be paid an all inclusive salary on Grade 7 and none of the allowances outlined in paragraphs 3.2.2-3.2.11 will apply. **No backdating of this all inclusive salary will apply.**

Part time Central Control Operators will receive a 34% enhancement on all hours worked in recognition of regular unsocial hours shifts worked on a Saturday/Sunday/Bank Holiday. This allowance will be removed following three months continuous absence. When covering for full time central control operators absence, the 34% enhancement will not apply.

Committee:	Union/Employee Consultation Committee	Agenda Item No.:	8.
Date:	12th March 2014	Category	*
Subject:	Sickness Absence/Occupational Health Statistics October to December 2013	Status	Open
Report by:	Joint Assistant Director – Human Resources		
Other Officers involved:	Human Resources Officer		
Director	Chief Executive Officer		
Relevant Portfolio Holder	Councillor E. Watts, Leader of the Council		

RELEVANT CORPORATE AIMS
STRATEGIC ORGANISATIONAL DEVELOPMENT – Continually improving our organisation by providing monitoring information which can be used to shape future policy decisions

TARGETS
The subject matter of this report does not contribute to any specific targets in the Corporate Plan.

VALUE FOR MONEY
As this report relates to retrospective monitoring data value for money criteria is not applicable

THE REPORT

1. Sickness Absence/Occupational Health Referral Statistics October to December 2013 compared to 2012.

   1.1 The sickness absence outturn for the third quarter of 2013/14 (October to December) is shown below, with comparisons for the same period during 2012/13:-

October to December 2012	October to December 2013
2.38 days per FTE	2.21 days per FTE

The target for October to December 2013 was 2 days per FTE. A breakdown of these figures by Department, and by long term/short term sickness absence, is attached for information.

Whilst the overall sickness absence figure shows a reduction the following should be noted:-

- Total number of days lost has reduced in 2013 by 212 days
- The number of days lost due to long term sickness has reduced in 2013 by 183.5 days
- The number of days lost due to short term sickness has reduced in 2013 by 28.5 days

1.2 The outcome of occupational health referrals for the third quarter of 2013/14, with comparisons for 2012 are shown below:

	October to December 2012	October to December 2013
Rehabilitated	4	5
Continuing	2	5
Ill Health	0	0
TOTAL	**6**	**10**

Continuing
2 employees (muscular/skeletal returned Jan 2014)
2 employees (stress/depression one returned Feb 2014)
1 employee (back/neck)
One muscular/skeletal employee was absent but we were not informed until October 2013 due to him triggering 20 days (long term sick)

1.3 A breakdown of the reasons for all long term sickness absence is as follows:

Reasons for Long Term Sickness Absence October to December 2013		
Reason for Absence	**No. of Employees Citing this Reason October to December 2012**	**No. of Employees Citing this Reason October to December 2013**
Back/Neck	-	3
Stomach/Digestion	2	-
Muscular/Skeletal	7	3
Sick/Other	1	1

Stress/Depression	6	2
Ear/Nose/Mouth	**-**	1
TOTAL	**16**	**10**

1.4 The following routine health surveillance clinics have been held during October to December 2013:

- 17th October 2013
- 7th November 2013

and covered topics such as

- Hand Arm Vibration
- Audiometry
- Driver medicals

There has been 1 employee undergoing counselling during this period.

ISSUES FOR CONSIDERATION

The report is for monitoring purposes only and there are no specific issues for consideration.

IMPLICATIONS

Financial : None
Legal : None
Human Resources : None

RECOMMENDATION(S)

1. The report be received.

ATTACHMENT: **Y (1)**
FILE REFERENCE: ***N/A***
SOURCE DOCUMENT: ***N/A***

BVPI12 - OCTOBER- DECEMBER 2013 OUT-TURN LONG TERM/SHORT TERM SPLIT

DEPARTMENT	AVERAGE EMPLOYEES 9 MTHS	DAYS LOST	FTE DAYS	LONG TERM ABSENCE NO OF DAYS	SHORT TERM ABSENCE NO OF DAYS	LT ABSENCE PER FTE	ST ABSENCE PER FTE
SENIOR MANAGERS GROUP	4.5	13	2.89	0.00	13.00	**0.00**	**2.89**
CHIEF EXECS DIRECTORATE	**4.5**	**13**	**2.89**	**0.00**	**13.00**	**0.00**	**2.89**
CHIEF EXECUTIVES AND PARTNERSHIP	4.50	7.5	1.67	7.50	0.00	**1.67**	**0.00**
STRATEGY/PERFORMANCE	8.15	5	0.61	0.00	5.00	**0.00**	**0.61**
HUMAN RESOURCES AND PAYROLL	6.50	1	0.15	0.00	1.00	**0.00**	**0.15**
DEMOCRATIC	7.04	4	0.57	0.00	4.00	**0.00**	**0.57**
LEGAL AND LAND CHARGES	8.69	5	0.58	0.00	5.00	**0.00**	**0.58**
RESOURCES DIRECTORATE	**34.88**	**22.5**	**0.65**	**7.50**	**15.00**	**0.22**	**0.43**
FINANCE	9.52	20	2.10	0.00	20.00	**0.00**	**2.10**
PROCUREMENT	1.81	0	0.00	0.00	0.00	**0.00**	**0.00**
CUSTOMER SERVICE	24.71	133.5	5.40	106.00	27.50	**4.29**	**1.11**
REVENUES	36.05	24.5	0.68	0.00	24.50	**0.00**	**0.68**
HEALTH AND WELL BEING	**72.09**	**178**	**2.47**	**106.00**	**72.00**	**1.47**	**1.00**
LEISURE	40.04	27	0.67	0.00	27.00	**0.00**	**0.67**
NEIGHBOURHOODS	**40.04**	**27**	**0.67**	**0.00**	**27.00**	**0.00**	**0.67**
COMMUNITY SAFETY	10.38	10	0.96	0.00	10.00	**0.00**	**0.96**
HOUSING (REPAIRS AND MANAGEMENT)	111.69	421.5	3.77	313.00	108.50	**2.80**	**0.97**
	122.07	**431.5**	**3.53**	**313.00**	**118.50**	**0.38**	**0.97**
STREET SERVICES	78.92	180.5	2.29	102.50	78.00	**1.30**	**0.99**
DEVELOPMENT							
PLANNING/HOUSING STRATEGY	17.85	3	0.17	0.00	3.00	**0.00**	**0.17**
REGENERATION	22.62	11	0.49	0.00	11.00	**0.00**	**0.49**
	40.47	**14**	**0.35**	**0.00**	**14.00**	**0.00**	**0.35**
GRAND TOTAL	***392.97***	***866.50***	***2.21***	***529.00***	***337.50***	***1.35***	***0.86***
Street Services include Depot Resources, Street Scene and Waste Services							
Housing includes Repairs and Maintenance and Supporting People Service							
Legal includes Land Charges							
Planning includes Housing Strategy							
Joint Directors included at 50%							
Joint Assistant Directors included at 50%							

Committee:	Union/Employee Consultation Committee	Agenda Item No.:	9.
Date:	12th March 2014	Category	*
Subject:	Equalities Monitoring Report October 2013 to December 2013	Status	Open
Report by:	Senior Human Resources Officer Human Resources Officer		
Other Officers involved:	Equalities Monitoring Report Human Resources Officer		
Director	Chief Executive Officer		
Relevant Portfolio Holder	Councillor E Watts, Leader of the Council Councillor A. Syrett, Portfolio Holder for Social Inclusion		

RELEVANT CORPORATE AIMS

SOCIAL INCLUSION – Promoting fairness, equality and lifelong learning
STRATEGIC ORGANISATIONAL DEVELOPMENT – Continually improving our organisation.

Ensuring that the Council has a framework in place for monitoring recruitment and selection, workforce breakdown, training, disciplinaries, grievances, labour turnover, efficiency and ill-health retirements by ethnic origin, gender, disability, age, sexual orientation and religion and pay and grading information in relation to market supplements, and appointments within the grade

TARGETS

Monitoring data will contribute towards Level 3 of the Local Government Equalities Standard

VALUE FOR MONEY

The monitoring of statistics/trends enables efficient and effective corrective action to be taken where necessary.

THE REPORT

To submit for Members attention monitoring data on the Council's performance on equalities issues in relation to its employment practices. This report does not cover corporate policy/service delivery monitoring.

It is recognised good practice to have a workforce that is broadly representative of the local community. With regard to the local community, the 2011 census provides the following information: -

1. The local population is 75,866, of which 37,442 are economically active.

2. An analysis of Bolsover District's population and workforce in respect of ethnicity is as follows:-

	White and White British	Mixed/ multiple ethnic groups	Asian/Asian British	Other	Black/African / Caribbean/ Black British
Population#	98.1%	0.7%	0.8%	0%	0.4%
Workforce##	99%	1%	0	0	0

#based on 2011 Census
##based on employee personal data as at 31st December 2013

3. An analysis of Bolsover District's population and workforce in respect of religion/beliefs is as follows:-

	Other	Christian	Hindu	Sikh	Buddhist	Muslim	Jewish	Prefer Not to Say	No Religion
Population#	0.3%	65.2%	0.1%	0.1%	0.2%	0.2%	0	6.8%	27%
Workforce##	1.40%	54.11%	0	0	0	0	0	27.05%	17.44%

#based on 2011 Census
based on employee personal data as at 31st December 2013

Performance Indicators

The following table identifies all performance indicators relevant to Equalities:-

INDICATOR	MEDIAN DERBYSHIRE AUTHORITIES 2011/12	AUTHORITY TARGET 2013/2014	AUTHORITY OUT-TURN OCTOBER TO DECEMBER 2013
HR11A - Percentage of top 5% of earners that are women	34.89%	45%	52.17%
HR11B - Percentage of top 5% of earners from black or ethnic communities	0%	0%	0%
HR11C - Percentage of top 5% of earners who are disabled	5.28%	7%	8.69%
HR16A - Percentage of disabled employees (permanent employees)	5.24%	6%	8.56%
HR17A - Percentage of employees from minority ethnic communities'	1.44%	0.50%	1.04%

Information and Analysis
Recruitment/Selection

Permanent Employees

For the period 1st October to 31st December, 2013 there were 9 vacancies, 118 applicants, 67 shortlisted and 18 successful applicants on one occasion there was more than one successful applicant for the vacancy (**i.e. 11 appointed Casual Leisure Attendant posts for the one vacancy advertised**). For the period 1st October to 31st December 2012 there were 8 vacancies advertised (two of which were unfilled), 65 applications received, 25 shortlisted and 12 successful candidates. On two occasions there was more than one successful candidate per vacancy.

Applicants Breakdown

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	94.92%	5.08%	77.96	22.04%	2.54%	25.42%	24.57%	29.67%	20.34%
2012	98.46%	1.54%	32.31%	67.69%	4.62%	20%	35.38%	24.62%	20%

Year	Heterosexual	Gay	Lesbian	Bisexual	Prefer Not to Say
2013	66.10%	0%	0%	0.85%	33.05%
2012	87.69%	0%	0%	0%	12.31%

Year	Christian	Buddhist	Hindu	Jewish	Muslim	Sikh	Any other	None/Prefer Not to Say
2013	80.50%	0%	0%	0%	0%	0%	0.85%	18.65%
2012	56.92%	0%	0%	0%	0%	0%	4.62%	38.46%

Shortlisted Candidates Breakdown

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	92.54%	7.46%	65.67%	34.33%	1.49%	22.39%	31.34%	23.88%	22.39%
2012	100%	0%	52%	48%	4%	16%	32%	40%	12%

Year	Heterosexual	Gay	Lesbian	Bisexual	Prefer Not to Say
2013	65.67%	0%	0%	0%	34.33%
2012	92%	0%	0%	0%	8%

Year	Christian	Buddhist	Hindu	Jewish	Muslim	Sikh	Any other	None/Prefer Not to Say
2013	61.19%	0%	0%	0%	0%	0%	2.99%	35.82%
2012	84%	0%	0%	0%	0%	0%	0%	16%

Successful Candidates

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	88.89%	11.11%	88.88%	11.11%	0%	44.44%	38.89%	16.67%	0%
2012	100%	0%	58.33%	41.67%	8.33%	16.67%	41.67%	33.33%	8.33%

Year	Heterosexual	Gay	Lesbian	Bisexual	Prefer Not to Say
2013	94.45%	0%	0%	0%	5.55%
2012	91.67%	0%	0%	0%	8.33%

Year	Christian	Buddhist	Hindu	Jewish	Muslim	Sikh	Any other	None/Prefer Not to Say
2013	94.45%	0%	0%	0%	0%	0%	0%	5.55%
2012	66.67%	0%	0%	0%	0%	0%	0%	33.33%

Workforce Monitoring

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	99%	1%	54.51%	45.49%	8.42%	7.02%	21.24%	31.86%	39.88%
2012	99.24%	0.76%	52.95%	47.05%	7.43%	11.05%	22.10%	30.09%	36.76%

Year	Heterosexual	Gay	Lesbian	Bisexual	Prefer Not to Say
2013	69.94%	0	0	0.20%	29.86%
2012	68.38%	0%	0%	0.19%	31.43%

Year	Christian	Buddhist	Hindu	Jewish	Muslim	Seikh	Any other	None
2013	54.11%	0	0	0	0	0	1.40%	44.49%
2012	52.19%	0%	0%	0%	0%	0%	1.33%	46.48%

Employee numbers are based on headcount @ 31st December 2013 with comparative figures @ 30th December 2012.

Training/Development

165 places have been 'taken up' with regard to off the job training. The breakdown of attendees is as follows:-

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	100%	0	67.88%	32.12%	5.45%	13.33%	20%	32.73%	33.94%
2012	99.02%	0.98%	51.47%	48.53%	6.37%	38.72%	16.18%	17.65%	27.45%

Year	Heterosexual	Gay	Lesbian	Bisexual	Prefer Not to Say
2013	61.82%	0	0	0	38.18%
2012	78.92%	0%	0%	0.49%	20.59%

Year	Christian	Buddhist	Hindu	Jewish	Muslim	Seikh	Any other	None
2013	45.46%	0	0	0	0	0	2.42%	52.12%
2012	46.08%	0%	0%	0%	0%	0%	2.45%	51.47%

Discipline

There were no disciplinary actions during this period.

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	0	0	0	0	0	0	0	0	0
2012	0	0	0	0	0	0	0	0	0

Grievances (including Harassment/Bullying)

There were no grievances lodged during this period.

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	0	0	0	0	0	0	0	0	0
2012	0	0	0	0	0	0	0	0	0

Labour Turnover

There have been 13 leavers during this period, the breakdown is as follows: -

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	100%	0%	76.93%	23.07%	15.38%	7.69%	15.39%	23.07%	53.85%
2012	100%	0%	50%	50%	8.33%	25%	16.67%	16.67%	41.66%

Voluntary Leavers
There have been 7 voluntary leavers during this period, the breakdown is as follows:-

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	100%	0	71.43%	28.57%	28.57%	14.29%	28.57%	0	57.14%
2012	100%	0%	42.86%	57.14%	0%	42.86%	28.58%	14.28%	14.28%

Dismissals
There was one dismissal on grounds of capability during this period, the breakdown is as follows:-

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	100%	0	100%	0	0	0	0	100%	0
2012	100%	0%	100%	0%	0%	0%	0%	0%	100%

Redundancies
There were 3 redundancies during this period, the breakdown is as follows:-

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	100%	0	66.67%	33.33%	0	0	0	0	100%
2012	100%	0	0%	100%	100%	0	0%	0%	100%

Ill-Health Retirements
There were no ill health retirement during this period.

Year	White	Ethnic	Male	Female	Disabled	16-24	25-39	40-49	50+
2013	0	0	0	0	0	0	0	0	0
2012	100%	0%	0%	100%	0%	0%	0%	0%	100%

ISSUES FOR CONSIDERATION
Analysis of the statistics/information presented/possible changes to policy to improve performance.

IMPLICATIONS
Financial - None
Legal - None
Environmental - None
Human Resources – None

RECOMMENDED that (1) the report be noted,
(2) recommendations be received as to improvements to current performance levels.

SOURCE DOCUMENTS: FILE REFERENCES: