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

INFORMATION SECURITY POLICY

June 2017

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)	ICT Manager
Location of policy – i.e. L-drive, shared drive	Within IT data drive
Member route for approval	Strategic Alliance Joint Committee/Executive/Cabinet
Cabinet Member (if applicable)	Cllrs Terry Connerton(BDC) and Jane Austen(NEDDC)
Equality Impact Assessment approval date	May 2013
Partnership involvement (if applicable)	
Final policy approval route i.e. Executive/ Council /Planning Committee	Strategic Alliance Joint Committee/Executive/Cabinet
Date policy approved	
Date policy due for review (maximum three years)	2020
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 Council 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 the 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. Member's 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 Services, partners, employees of the Council, Rykneld Homes Ltd and other stakeholders such as contractual third parties, agents, work placements, where they have access to ICT facilities.

These policies are produced in line with guidelines and legislation that are available as of February 2017. These include:

2.1 Legislation and guidelines:

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 and, from May 2018, the General Data Protection Regulations- 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.

Information Commissioners Office (ICO) General Data Protection Regulations Guidance 1.0. This expands on the Data Protection 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.

Local Public Services Data Handling Guidance covers Central Government produced data and documents and is now being adopted more widely. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370725/PSN_local_public_services_data_handling_guidelines.pdf

Public Services Network (PSN) Code of Connection. This is a requirement to access central government provided services and a comprehensive list of conditions must be met to achieve the requisite compliance.

3 Principles

This document provides a summary of the information security policies developed by the Council and Rykneld Homes Ltd. The objective of these policies is to ensure the highest standards of information security are maintained across the Councils and Rykneld Homes at all times so that:

- Duties are carried out in a professional and lawful manner and in accordance with the Councils and Rykneld Homes Ltd Codes of Conduct.
- The public and all users of the the Council 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 Councils and Rykneld Homes ICT equipment and facilities are used responsibly, securely and with integrity at all times.

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 Procedures.

It is intended that from time to time, as is required by changes to legislation, technology or the Councils' or Rykneld Homes policy, these Guidelines will be subject to review. Any changes made will be subject to consultation and the changes communicated to users. By signing the agreement users are deemed to accept any revisions to this policy that are communicated to them.

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 Councils or Rykneld Homes and may result in financial loss and an inability to provide services to our customers.

5 Information Security Policy

The detailed policies that are attached as appendices include:

- Protective Marking Policy
- 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 above 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 Document Classification and Protective Marking Policy (Appendix 1)

Many organisations have formal documentation classification schemes. We have a responsibility to ensure we are aware of the data handling guidelines in relation to these documents or data. For these purposes documents are either paper whereas data is held in a business system database or as a raw data extract on Council filing systems. Electronic documents would usually be created using part of the Microsoft Office suite or in 'pdf' format but other forms may also exist. If in doubt always seek clarification from the data owner or your line manager.

The Government adopted a new classification scheme in 2014 and the Council has adopted this scheme. We should not receive any material classified as SECRET or TOP SECRET, any material classified as thus should be immediately deleted and the sender

notified. There are two classifications that will apply to each organisation: OFFICIAL and OFFICIAL SENSITIVE:

- OFFICIAL-SENSITIVE Broadly this includes data or documents that contain personal or personal sensitive data as defined by the Data Protection Act or defined under 'Special categories' under the General Data Protection Regulations. This can also include items that would be considered exempt under the Freedom of Information Act in relation to commercial sensitivity.
- OFFICIAL Covers all other documents and data that do not fall under the OFFICIAL-SENSITIVE classification and will form the majority of the Councils data and documents

A full definition of the Government Classification Scheme can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

Key points to note:

- New documents which contain personal sensitive data as defined by the Data Protection Act or fall within a 'Special Category' under the General Data Protection Regulations should be protectively marked as OFFICIAL-SENSITIVE on both the header and footer of each page
- Amended documents should be protectively marked where not already marked
- Transmission of OFFICIAL-SENSITIVE material should be clearly marked as thus and appropriate steps taken to ensure transmission is secure
- Care should be taken with unmarked documents

Under the Data protection Act the following are defined as personal sensitive data:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Under the General Data Protection Regulations in place from May 2018 the following are defined as 'Special Categories' of data or are covered elsewhere in the Regulation:

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs

- Trade Union membership
- Genetic data
- Biometric data
- Sex life or sexual orientation
- Physical and mental health
- Financial personal data
- Alleged criminal activity
- Criminal record

5.2 Email (Appendix 1)

- The use of email facilities will be permitted only by users that have been specifically designated as authorised users, received appropriate training and have confirmed in writing they accept and agree to abide by the terms of this policy.
- All emails that contain OFFICIAL-SENSITIVE information should be encrypted in transit when sent to other organisations whether in the public sector or not, see secure email guidance available on the Joint ICT Service intranet. Please contact the Joint ICT Service Desk if you are unsure if the recipient can receive secure email.
- Where correspondence is made directly with members of the public that contains OFFICIAL-SENSITIVE information it is not possible to ensure emails can be encrypted but all precautions to ensure the email address belongs to the intended recipient should be made.
- All correspondence which contains OFFICIAL-SENSITIVE material should be marked as such in the email title.
- 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.
- Email should not be forwarded to personal email accounts under any circumstances.
- Auto forwarding of email to email addresses outside of the Council & Rykneld Homes Ltd is not permitted.
- 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 the Council & Rykneld Homes Ltd business should be considered to be an official communication from the council or Rykneld Homes.
- The Council and Rykneld Homes Ltd maintain their 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. The Council and Rykneld Homes Ltd reserve the right, with written approval from an appropriate Director, Assistant Director or the Human Resources & OD Manager, to monitor emails sent within the Council and Rykneld Homes email system…. without further notifying the individual concerned that the right is being exercised. Please see Appendix 1, specifically section 3.1, for further clarification on this issue.

- 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.

5.3 Internet Acceptable Usage (Appendix 2)

- Internet use is monitored by the Council 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.

5.4 Software (Appendix 3)

- All software acquired must be approved by the ICT Manager of the Joint ICT Service or their deputy.
- 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 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 Council 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.

5.5 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 user 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 Joint ICT Service before connecting to the Bolsover District Council, North East Derbyshire District Council or Rykneld Homes Ltd. network.

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

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

5.7 Human Resources Information Security Standards (Appendix 6)

- All employees are expected to adhere to this policy
- Access to Information systems must be relevant to the jobholders role and duties
- All mandatory ICT training should be completed in a timely manner or access to systems will be removed
- In addition to normal recruitment verification checks carried out on all new employees' additional checks may be required, primarily when accessing systems and data provided by 3rd parties.

5.8 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 Government Security Classification scheme..
- 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.
- OFFICIAL-SENSITIVE information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing OFFICIAL-SENSITIVE classified information to any external organisation is also prohibited, unless via secure email.
- The disclosure of OFFICIAL-SENSITIVE information other than for approved purposes is a potential breach of the Data Protection Act and should be reported to the internal Data protection team.

5.9 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. OFFICIAL-SENSITIVE information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

5.10 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. Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- All OFFICIAL-SENSITIVE data held on portable computer devices must be encrypted.

5.11 Removable Media (Appendix 10)

- The use of all removable media devices such as USB memory sticks, data cards and writeable CD's and DVDs is prohibited unless a business case is agreed, training 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 General Data Protection Regulations and report any suspected breaches.

5.12 Information Security Incident Management (Appendix 11)

- All users should report any incidents or suspected incidents immediately by contacting the Joint ICT Service.
- 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. The Data Protection team should be contacted for guidance.
- Users should be aware of their responsibilities in regard to the Data Protection Act and report any suspected breaches.

5.13 ICT Infrastructure Security (Appendix 12)

- OFFICIAL-SENSITIVE 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. OFFICIAL-SENSITIVE 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**.

5.14 Data Protection

- All employees are expected to adherence to the Council's and Rykneld Homes Data Protection practices and the specific policies listed supports compliance with the Data Protection Act 1998 and reduces the risk of data protection breaches.
- Full details and guidance are available on the Data Protection pages on the Council and Rykneld Homes intranets.

5.15 Business Continuity

Electronic information assets are protected to ensure the Councils and Rykneld Homes business can continue in the event of significant physical disruption to one or more of the main Council and Rykneld Homes sites. This includes:

- Physical security, arms and fire suppressant at main data centres
- Daily replication of data to designated disaster recovery sites for data managed by the Joint ICT Service
- Daily backups of data held offsite for data managed by the joint ICT Service. This data is retained for 30 days
- Corporate business continuity plans

5.16 Disposal and Destruction of Data

- Confidential waste bins are provided for the secure destruction of paper based records
- All unused electronic devices should be returned to the Joint ICT Service when no longer in use.
- All Council electronic data devices and removable are disposed of by the Joint ICT Service in accordance with regulation and for removable media and hard disks are destroyed to DOD 5220-22M standard
- Please refer to the Council or Rykneld Homes Corporate Retention & Disposal Schedules

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 Officers, 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 the Council will support any action 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 complying with the policy would breach Health and Safety.

- 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.

- 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.

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 the 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 the Councils & Rykneld Homes Ltd for the purpose of conducting and supporting official business activity through the , The 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 Services, partners, employees and individuals working on behalf of the Councils & 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 Public Service Network Code of Connection.

References to protective marking schemes and guidance on assessing and handling such information are covered in Section 5.1 of the Information Security Policy

3. Email Policy

3.1 Email as Records

- All emails that are used to conduct or support the councils 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.
- 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.
- For OFFICIAL-SENSITIVE information encryption **should** be used for all content and/or attachments that contain that classification. Secure email guidance is available on the Joint ICT Service Intranet.
- Where secure email is **not** available to connect the sender and receiver of the email message, and information classified as OFFICIAL-SENSITIVE is being transferred, alternative encryption methods **must** be used for all content and/or attachments that contain that classification. The ICT Service Desk will advise on options available.
- Emails carrying OFFICIAL-SENSITIVE 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 "OFFICIAL-SENSITIVE" as appropriate.
- Auto forwarding of email to email addresses outside of the Council & Rykneld Homes Ltd is not permitted.
- Automatic forwarding of email within the organisations email system must be considered carefully to prevent OFFICIAL-SENSITIVE material being forwarded inappropriately.
- When handling data and documents provided by a 3rd party any document handling guidance provided by the 3rd party should be observed.

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 Council emails containing OFFICIAL-SENSITIVE information must be sent via secure email. All emails that represent aspects of Councils & Rykneld Homes Ltd business or Council & Rykneld Homes Ltd administrative arrangements are the property of Council or Rykneld Homes Ltd., as appropriate, and not of any individual employee.

Emails held on Councils & 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 Councils & Rykneld Homes Ltd business should be considered to be an official communication from the council or Rykneld Homes. In order to ensure that 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, the 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 Assistant Director or the Human Resources & OD 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 approval from an appropriate Director, Assistant Director or Human Resources & OD 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.
- disclosure under the Data Protection Act 1998 or the Freedom of Information Act 2000.

In these circumstances you do not have a right to privacy when using the Councils & Rykneld Homes Ltd's information systems or in relation to any communication generated, received or stored on the Councils & 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 OFFICIAL-SENSITIVE information or of communicating in the particular circumstances.

All emails sent to conduct or support official 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 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 Councils & Rykneld Homes Ltd's Equal Opportunities Policies, 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 the 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 OFFICIAL-SENSITIVE material concerning the activities of the Councils & 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 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 the Council or Rykneld Homes Ltd into disrepute.

3.3 Unsolicited 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 or opening any attachments or hyperlinks. 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 Council or Rykneld Homes Ltd systems or facilities.

3.4 Mail Retention

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.

Whilst there are no limits on mailbox sizes emails will be archived after 3 months and deleted after 2 years. This applies at the Councils only, mailbox limits currently apply at Rykneld Homes Ltd.

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.

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 the 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.
g. 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.

Where a manager suspects that the email facilities are being abused by a user, they should contact the ICT Manager and HR. Designated staff in the Joint ICT Service can provide evidence and audit trails of access to systems. The Joint ICT Service 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 the latter is the case the Councils or Rykneld Homes Ltd may exercise this right, with approval from an appropriate Director, Assistant Director or the Human Resources & OD Manager. 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 Classification of Messages

The Council has adopted the Government protective marking scheme. However we may handle data on behalf of 3rd parties who, as data owners, have adopted different protective marking schemes and data handling guidance. Please refer to section 5. Of the Information Security Policy for further information.

3.7 Secure email

Emails sent between:

ne-derbyshire.gov.uk,

rykneldhomes.org.uk,

- bolsover.gov.uk and

derbyshiredales.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, Council OFFICIAL-SENSITIVE material must not be sent via email unless assured as secure.

Where secure 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 OFFICIAL-SENSITIVE material.

Where secure email is not available to connect to the receiver of the email message, and information classified as OFFICIAL-SENSITIVE is being transferred, encryption should be used for all content and/or attachments that contain that classification. Please contact the Service Desk if the you are unsure if the recipient can receive secure email.

Emails carrying OFFICIAL-SENSITIVE 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 “OFFICIAL-SENSITIVE” (with appropriate descriptor) as appropriate.

Please refer to the secure email guidance available on the Joint ICT Service Intranet.

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 the Council or Rykneld Homes Ltd.

Care should be taken when addressing all emails, but particularly where they include OFFICIAL-SENSITIVE 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 OFFICIAL-SENSITIVE 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.

3.9 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. If any user has concerns about possible virus transmission, they must report the concern to the Joint ICT Service and under no circumstances forward emails and attachments or open links in an email if there is any cause for concern.

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 Council 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 Council and Rykneld Homes use for research and education purposes. Internally, the Council and Rykneld Homes have also developed Intranet sites (e*ric*, 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 Council and Rykneld Homes setting. Additionally, as with any resource, there is the possibility of misuse. Accordingly, the Council and Rykneld Homes need 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.

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of the Councils & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who make use of the internet.

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, e.g. 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 a member of the senior management team.

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.

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 the 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 the Councils 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 Council 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 Joint ICT Service 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 Services, partners, employees of the Council & Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who make use of ICT equipment.

3. Software Policy

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

3.1 Software Acquisition

All software acquired by the Council and Rykneld Homes Ltd. may only be purchased following consultation with the joint ICT service and approval provided by the ICT Manager or his deputy. 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.. 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 Council or Rykneld Homes machine as this may affect the performance of your device and the 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 the 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 Joint ICT Service maintains a register of all 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.

The Council and Rykneld Homes Ltd. holds licences for the use of a variety of software products on all Council 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 Joint ICT Service once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by the Joint ICT Service.

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 Joint ICT Service

To maintain PSN compliance and to mitigate the risk of security vulnerabilities on version of software that are supported by the manufacturer of that software will be permitted. Where applicable a current support and maintenance agreement with the application provider should be in place.

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 and approved by the ICT Manager of the Joint ICT Service. 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.

4.6 Software Misuse

The Council and Rykneld Homes Ltd. will ensure that Firewalls and anti virus products are installed where appropriate. Users **must not** attempt to disable or reconfigure the Firewall or anti-virus software.

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

According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any individual, who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under the circumstances. Any illegal duplication of software may be treated as a disciplinary offence.

APPENDIX 4 - ICT ACCESS POLICY

1. Introduction

Access control r**u**les and procedures are required to regulate who can access 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 Council or or Rykneld Homes 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 Services, partners, employees of the Council Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who access ICT services.

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.

Strong passwords should be used 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 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 Joint ICT Service.

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

5. System Administration Standards

All Council and Rykneld Homes 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 Joint ICT Service for approval. Applications for access must only be submitted if approval has been gained from your line manager.

When a user leaves the Council 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 Joint ICT Service and te relevant business system administrators.

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 Joint ICT Service and the relevant business system administrators of any changes to their role and access requirements.

6.3 Network Access Control

Connecting non Council devices to the Council or Rykneld Home networks is strictly forbidden without prior approval and risk assessment by the Joint ICT Service.

7. Users Authentication for External Connections

Where remote access to the the Council Rykneld Homes network is required, an application must be made to the Joint ICT Service. 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 Joint ICT Service. Any changes to supplier's connections must be immediately sent to the Joint ICT Service so that access can be updated or ceased. All permissions and access methods must be controlled by the Joint ICT Service.

Partners or 3rd party suppliers must contact the Joint ICT Service before connecting to the Council or Rykneld Homes 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 the Council and Rykneld Homes, contractual third parties and agents, work experience and volunteers.**3. Principles**

It is the Councils and 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 Council and Rykneld Homes information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Council and Rykneld Homes 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 OFFICIAL sent via the PSN; and,
xii. I will not send OFFICIAL-SENSITIVE information over unsecured public networks such as the Internet; and,
xiii. I will always check that the recipients of e-mail messages are correct so that OFFICIAL-SENSITIVE 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 secure-email account; and,
xv. I will not forward or disclose any OFFICIAL-SENSITIVE 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 OFFICIAL-SENSITIVE 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 and 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 or tablet 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 General Data Protection Regulations 2018 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 services provided via PSN. 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 Council, 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.

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 Services, partners, employees of the 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

The 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 relevant to the jobholders role and duties.
- 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 Joint ICT Service 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.

ICT staff with network administration rights and, where appropriate or required by 3rd party agreements, will also require standard checks through the Disclosure and Barring Service.

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).

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.

Service 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 of ICT systems are required to undertake n security awareness training and should take note of updates in related statute and organisational policies and procedures as relevant for their role.

It is the role of Service 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 Council and Rykneld Homes 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, tablets, 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 the 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 the 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

The 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, mobile devices, removable media).
- 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 personal data 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 Data Retention

The Council and Rykneld Homes LTD have data retention policies in place.

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 OFFICIAL-SENSITIVE Information with other Organisations

OFFICIAL-SENSITIVE 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.

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

The disclosure of OFFICIAL-SENSITIVE information in any way other than via secure email is a disciplinary offence. If there is suspicion of a user treating OFFICIAL=SENSITIVE 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 OFFICIAL-SENSITIVE 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 the Council and Rykneld Homes Ltd, contractual third parties and agents, work experience and volunteers who have access to information systems or information used for Council and Rykneld Homes purposes.

3. Principles

This policy should be applied whenever users who access information systems or information utilise Council and Rykneld Homes computer and telephony resources.

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

- Centralised server and storage systems
- Hosted solutions(Cloud)
- Personal computers.
- Portable laptop computers.
- Removable media (memory cards and sticks)
- Mobile devices(smart phones, tablets)
- 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

The 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 desks should, wherever possible, be cleared of all documents that contain any protectively marked documents as per the classification scheme of the Council or data owner 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 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.

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 the Council & Rykneld Homes, contractual third parties and agents, work experience and volunteers who use Council and Rykneld Homes Ltd IT facilities and equipment when working on official business away from the organisation (i.e. working remotely), or who require remote access to Council and Rykneld Homes Ltd information Systems or information.

3. Principles

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.
- Mobile phones.
- Wireless technologies.

4. Applying the Policy

All IT equipment (including portable computer devices) purchased for users by the Council or Rykneld Homes is the property of the purchaser. It must be returned upon the request of the purchaser. 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 gcsx email, **under no circumstances** should non-Council owned equipment be used.

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 the North East Derbyshire District Council ICT department.
- Users will allow the installation and maintenance of Council and Rykneld Homes Ltd installed Anti Virus updates immediately.
- Users will inform the Joint ICT Service 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 Joint ICT Service.
- Users must not remove or deface any asset registration number.
- Users registration must be requested from the Joint ICT Service. 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 the ICT Service. 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, 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.
- The Council and Rykneld Homes Ltd. may at any time, and without notice, request software and hardware audits, 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 OFFICIAL-SENSITIVE 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 users accessing PSN services or facilities, or using OFFICIAL-SENSITIVE 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

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. All documents classified as OFFICIAL-SENSITIVE must be disposed of via confidential waste facilities.

7. Access Controls

It is essential that access to all OFFICIAL-SENSITIVE 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 OFFICIAL-SENSITIVE 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.

Only methods approved and provided by the Joint ICT Service must be configured to allow remote access to the councils or Rykneld Homes systems if connecting over Public Networks, such as the Internet.

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 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

All Council devices have anti virus protection. Under no circumstances should this be disabled or modified.

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.

All users must have attended mandatory Security Awareness Training and Data Protection training.

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 OFFICIAL-SENSITIVE information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection the 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 Council or Rykneld Homes information systems or IT equipment and intends to store any information on removable media devices.

3. Principles

The Council and Rykneld Homes 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

The Council and Rykneld Homes 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 OFFICIAL-SENSITIVE 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 Council or Rykneld Homes. It is therefore essential for the continued operation of the Council 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 the Council and Rykneld Homes 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 significant 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 a Service 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 Joint ICT Service 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 OFFICIAL-SENSITIVE 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 Joint ICT Service 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 Joint ICT Service ICT Manager and the Data Protection Officer.

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 Joint ICT Service should removable media be damaged and return to ICT for secure disposal.

Virus and malware checking software approved by the Joint ICT Service 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 the Joint ICT Service for secure disposal**.

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

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:

- 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 Council or Rykneld Homes 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 Council or Rykneld Homes 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 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 Joint ICT Service in order to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the Joint ICT Service 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 Joint ICT Service 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 the Joint ICT Service. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by the Joint ICT Service.

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 Joint ICT Service 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 Corporate Risk Impact Methodology.

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 Council 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 the Council and Rykneld Homes 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 Council and Rykneld Homes Ltd. information equipment and information must be protected.

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 the Council and Rykneld Homes contractual third parties and agents, work experience and volunteers who have access to Council or Rykneld Homes 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:

- IT equipment that hold Electronic data
- 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 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

OFFICIAL- SENSITIVE 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 Service 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 Service, 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.

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.
- If laptops or tablets must be left at the office overnight then they should be kept out of sight, preferably in a locked drawer or cabinet
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs and laptops 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, maintained by ICT. 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 ICT inventory.

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

Please refer to the Remote Working Policy.

9. Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must be returned to the Joint ICT Service 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.