Committee:	Union Employee Consultation Committee	Agenda Item No.:	3.
Date:	7th January 2009	Category	
Subject:	Review of IT Security Policy	Status	Open
Report by:	Senior IT Projects Officer		
Other Officers involved:			
Director	Director of Resources		
Relevant Portfolio Holder	Portfolio Holder for Corporate Efficiency		

RELEVANT CORPORATE AIMS

COMMUNITY SAFETY – Ensuring that communities are safe and secure
CUSTOMER FOCUSED SERVICES – Providing excellent customer focused services
ENVIRONMENT – Promoting and enhancing a clean and sustainable environment
REGENERATION – Developing healthy, prosperous and sustainable communities
SOCIAL INCLUSION – Promoting fairness, equality and lifelong learning.
STRATEGIC ORGANISATIONAL DEVELOPMENT – Continually improving our organisation.

The policy either directly or indirectly supports the corporate aims by ensuring that safeguards are in place to reduce the risk of ICT service disruption by accidental or malicious acts, thus allowing Departments to meet their commitments to these aims.

TARGETS

This does not directly contribute to any targets specified in the Corporate Plan.

VALUE FOR MONEY

The policy does not directly deliver value for money for the Council and its customer.

THE REPORT

The IT security policy is reviewed on a regular basis; this particular review has been driven by the need to meet the code of connection for Government Connect. The Department for Work and Pensions is withdrawing its current method for data exchange from 1st April 2009 and mandating that all Authorities must use Government Connect for the secure exchange of data.

Changes to the policy are highlighted in italics, they include:

- Additional awareness training for employees who will be accessing restricted information.
- Change to the way that employees are able to work from home, in future anything other than simple email access will have to be done from an Authority supplied laptop.
- Employees at home will also be required to have a Crypto Card which increases the level of security when they login.
- Requirement to use BCC option when sending mail to groups where the mailing list contains personal sensitive information.
- Removable media containing personal data must be encrypted.

Training sessions will take place for all employees and elected Members during 2009 highlighting the changes and reinforcing the need for ICT security.

ISSUES FOR CONSIDERATION

Whether to accept the revised policy.

IMPLICATIONS

Financial :	Costs to meet the changed requirements are being met from existing budgets or part of the budget bid process for 2009/2010.
Legal :	None
Human Resources :	Home working policy may need to be revised.

RECOMMENDATION(S)

To accept the revised ICT security policy.

ATTACHMENT:	**Y**
FILE REFERENCE:	sups/computer/policies_strategies_and_plans
SOURCE DOCUMENT:	IT security policy under review

BOLSOVER DISTRICT COUNCIL

Information Management

And

Information Communications Technology

Security Policy

July 2008

DRAFT

This Policy addresses the following Corporate Aims:

The District of Bolsover Equalities Statement

Bolsover District Council is committed to equalities as an employer and in all the services provided to all sections of the community.

The Council believes that no person should be treated unfairly and is committed to eliminate all forms of discrimination in compliance with the Equality Strategy.

The Council also has due regard to eliminate racial discrimination and to proactively promote equality of opportunity and good relations between persons of different racial groups when performing its functions.

This document is available in large print and other formats from any of the Council offices or by contacting the Chief Executives Directorate on 01246 242323. Please bear in mind we will need a few days to arrange this facility.

If you need help to read this document please do not hesitate to contact us.

Our Equality and Improvement Officer can be contacted via **Email** or by telephoning 01246 242407.

Minicom: 01246 242450
Fax: 01246 242423

DATA PROTECTION
Information given to Bolsover District Council will be used only for the Council's lawful purposes, for the provision of joined up services, and will not be passed to anyone outside the Council without lawful Council.

DRAFT

Details of Document	
Title	Information Management and Information Communications Technology Security Policy
Document type – i.e. draft or final version	Draft
Location of Policy	L:sups/computer/policies, strategies and plans/IT security policy
Author of Policy	Senior IT Projects Officer
Reviewed by Director of Strategy.	9/10/08
Risk Assessment completed	20/11/08
Community Safety implications	None
Equality Impact Assessment completed.	20/11/08 submitted
Approved by	Executive
Date Approved	
Policy Review Date	

DRAFT

CONTENTS

DRAFT

1. Introduction

The aim of this policy is to ensure that information and ICT assets are protected from accidental and malicious acts such as destruction, theft and unauthorised disclosure which could cause distress or harm to individuals, other organisations or to the Council and/or would be in breach of legislative, regulatory and contractual requirements.

This policy has been adapted from the British Standard Code of Practice for Information Security Management BS ISO/IEC 27001.

The policy is also intended to act as a Corporate Information Risk Policy.

Risk assessment and management of risk is dealt with in the following documents issued by the Business Risk Group:

- **Bolsover Council Risk Management Strategy**
- **Risk Management Summary Guidance Notes**
- ***Data Quality Management Statement***
- ***Data Protection Code of Practice***

These documents are to be adhered to when ascertaining the risk to assets, information, personnel and systems connected with the daily business activities of Bolsover District Council

2. Scope of the Policy

This policy is applicable at all the Council offices, at any location where Council ICT assets are in use or connected to remotely from non-council ICT assets. This policy also applies to third parties who are employed or contracted to work with Bolsover District Council and whom have access to information or ICT assets.

DRAFT

3. Principles of the Policy

This policy directly supports the following Corporate Aims:

Customer Focused Services by linking the requirements of the Customer Service Code of Practice and Standards with the requirement to reduce the risk of malicious attack, thereby allowing the Council to continue to provide excellent customer focused services.

Strategic Organisational Development by providing best practice guidelines in order that we can continually improve our organisation.

Indirectly this policy supports the remaining Corporate Aims by ensuring safeguards are in place to reduce the risk of ICT service disruption by accidental or malicious acts, thus allowing Services to meet their commitments to these aims.

Community Safety

Environment

Regeneration

Social Inclusion

DRAFT

4. The Policy

The purpose of this policy is to:

Safeguard ICT assets and the information belonging to the Council.

Ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

Enable information to be shared whilst ensuring the protection of information and ICT assets.

Provide management direction and support for information security.

This policy adopts the eleven security clauses of BS ISO/ IEC 27001. which are:

- The Security Policy
- Organising Information Security
- Asset Management
- Human Resources Security
- Physical and Environment Security
- Communications and Operational Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

There are three basic components to information security management, it is characterised by the preservation of:

Confidentiality - Ensuring that information is accessible only to those authorised to have access.

Integrity - Safeguarding the accuracy and completeness of information and processing methods.

Availability - Ensuring that authorised users have access to information and associated assets when required.

DRAFT

4.1 **The Security Policy**

The objective is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

4.1.1 Infringements of Policy

Infringements of this Policy may warrant disciplinary action or instigation of the members' complaint procedure and, in cases of gross misconduct by employees, may result in termination of employment. When necessary the Police will be informed. In particular, attention is drawn to the following infringements:

4.1.1.1 Viewing, creating, circulating, distributing, storing, downloading or printing material that might be offensive, illegal, pornographic or sexually explicit, that brings the Council into disrepute or that exposes it to legal action. For employees, such action is likely to be considered as gross misconduct and, if so, could result in termination of employment without notice. For members, this will instigate the Members' Complaint Procedure. The Council reserves the right to recover defamatory material and use it as evidence against an individual.

4.1.1.2 Using communication facilities for purposes that may be illegal or contravene Council policy such as disclosing official information without Council.

4.1.1.3 Hacking, hoaxing, damaging Council or other networks or knowingly using unlicensed software.

4.1.1.4 Using the Council email system to send personal e-mails without permission.

4.1.1.5 Using communication facilities for private use during working hours.

DRAFT

4.2 **Organising Information Security**

The objective is to manage information security within the Council.

4.2.1 Information security activities should be co-ordinated by representatives from different parts of the Council with relevant roles and job functions.

4.2.1.1 Information security is a responsibility shared by all elected members and employees of Bolsover District Council.

4.2.1.2 The management and implementation of information security controls is co-ordinated throughout the Council by the Head of ICT.

4.2.1.3 Risk assessment and treatment is managed by the Head of ICT and co-ordinated by the Business Risk Group.

4.2.1.4 The Senior IT Projects Officer shall have procedures in place identifying how to handle non-compliance.

4.2.1.5 The IT Training Officer shall effectively promote information security education, training and awareness throughout the Council.

4.2.1.6 The Senior IT Projects Officer shall evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents.

4.2.1.7 The Senior IT Projects Officer shall ensure that the Data Protection Officer is informed of any security incidents that involve customer or employee data.

4.2.2 All information security responsibilities should be clearly defined.

4.2.2.1 The software and hardware register shall include details of asset ownership.

4.2.2.2 An overall owner for each system, an Information Asset Owner, shall be in place and that owner is responsible for its day to day protection.

4.2.2.3 *Information Asset Owners* shall clearly define and document the authorisation levels they allow.

4.2.3 A management authorisation process for new information processing facilities should be defined and implemented.

4.2.3.1 The IT Strategy Group shall be responsible for authorising all new information processing facilities.

DRAFT

4.2.3.2 The IT Support Officer shall have a procedure for authorising all new users of information processing facilities.

4.2.3.3 The use of personal or privately owned information processing facilities for the processing of business information is forbidden. *They may only be used for accessing email.*

4.2.3.4 The use of personal or privately owned information processing facilities for the processing of business information that has a protective marking of RESTRICTED is forbidden.

4.2.4 Requirements for confidentiality or non-disclosure agreements reflecting the Council's needs for the protection of information should be identified and regularly reviewed.

4.2.4.1 Staff and Members may be required to sign non-disclosure agreements before being granted access to Council information.

4.2.4.2 Terms shall be included in employment contracts requiring assets including information to be returned or destroyed at the end of the contract.

4.2.4.3 Employees who handle RESTRICTED information are required to confirm their acceptance that communications sent or received via the GSi may be intercepted or monitored.

4.2.4.4 Employees who handle RESTRICTED information shall be given additional security training to ensure that they understand the impact of the loss and the procedures to be followed in the event of any such loss.

4.2.4.5 Blind copying must be used on group emails involving members of the public e.g. sending citizens panel surveys out electronically. Internally this also applies to the Union as trade union membership is personal sensitive data under the DP Act and should not be shared amongst other employees.

4.2.5 Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

4.2.5.1 The Senior IT Technical Officer shall be the nominated contact for the regional WARP.

4.2.5.2 Vendors websites shall be monitored on a regular basis to check for security incidents.

4.2.6 The Council's approach to managing information security and its implementation should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

DRAFT

4.2.6.1 The *Head of IT* shall arrange independent audits of information security; *the recommendations will be referred to the IT Strategy group*.

4.2.6.2 The internal audit function shall include audits of controls, processes and procedures for information security within their audit plan.

4.2.7 The risks to the Council's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before giving access.

4.2.7.1 A verification procedure shall take place before access is granted to the network by third parties.

4.2.7.2 Physical access to Sherwood Lodge and the Depots shall be restricted by the core key system.

4.2.7.3 Physical access at Contact Centres shall be restricted by key pads. The numbers shall be changed when employees with access to the numbers leave and on a regular basis, at least six monthly.

4.2.7.4 Access to the machine rooms at Sherwood Lodge shall be limited to the following posts within IT and to specific posts that have a responsibility for building maintenance:

Head of ICT

Senior First Line Support Officer

Senior Second Line Support Officer

Senior IT Projects Officer

IT Technical Officer

Network and Infrastructure Officer

Network and Telecommunications Officer

IT Support Officer

.

DRAFT

4.3 **Asset Management**

The objective is to achieve and maintain appropriate protection of Council assets. All assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

4.3.1 All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

4.3.1.1 A software and a hardware register shall be maintained by the IT Support Officer.

4.3.1.2 Information recorded against each asset shall include the type of asset, format, location, backup information, license information, nominated owner and a business value.

4.3.1.3 An annual physical audit of all hardware and software assets shall be undertaken by the IT Support Officer.

4.3.1.4 All software shall be stored within the ICT Service, it's installation controlled by procedures.

4.3.1.5 Assets may only be used for authorised business purposes.

4.3.2 Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented and implemented.

4.3.2.1 All Members, employees and third party users must follow the rules for acceptable use as defined in:

- Employees Code of Conduct .
- *Email and Internet Policy October*.
- Computer User Handbook for Members and Employees.

4.3.2.2 Monitoring of acceptable use will take place and procedures shall be in place for dealing with breaches of any the above policies.

4.3.3 Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the Council. The classification and associated protective controls for information are to:

- Take into consideration the business need for sharing or restricting information and the business impacts associated with these needs.

DRAFT

- Ensure the conventions for the initial classification and reclassification over time take place and that the appropriate means of labelling and despatch are used.
- Ensure compliance with legal requirements such as Data Protection Act, Freedom of Information Act and Financial Regulations.

4.3.3.1 Each Head of Service is responsible for the safeguarding of information under the control of their Service and to ensure that their employees are aware of their responsibilities when handling restricted or sensitive information.

4.3.3.2 Paper Information shall be disposed of by shredding.

4.3.3.3 Magnetic and optical media shall be returned to ICT Services for safe disposal

4.3.3.4 ICT equipment is to be securely wiped of all information prior to disposal.

4.4 **Human Resources Security**

The objective is to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk to theft, fraud or misuse of facilities.

4.4.1 Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with this policy.

4.4.1.1 Security roles and responsibilities shall be defined and clearly communicated to job candidates during the pre-employment process.

4.4.2 Background checks prior to employment, such as references, confirmation of ID, or criminal records, and confirmation of academic and professional qualifications should take place.

4.4.3 Users of the network who are able to connect to GCSX and have regular access to RESTRICTED information or information that originates from the GSi must be cleared to the "Baseline Personnel Security Standard"

4.4.4 As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the Council's responsibilities for information security.

4.4.4.1Any Home working Policy shall state the responsibilities that are extended to those working outside the Council's premises and outside normal working hours.

DRAFT

4.4.4.2 The terms and conditions of employment shall state the actions to be taken if the employee, contractor or third party user disregards the Council's security requirements.

4.4.5 During employment, management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the Council.

4.4.5.1 All employees, contractors and third party users who require computer access shall receive security awareness training as part of the formal induction process.

4.4.5.2 The security awareness training shall include legal responsibilities, business controls as well as training in the correct use of information processing facilities, e.g. logon procedures, use of software packages and information on the disciplinary procedure. *Additionally it will cover data handling and an awareness of how to handle personal data.*

4.4.5.3 Additional security awareness training regarding loss of data and the actions to be taken will be given to u*sers of the network who are able to connect to GCSX and have regular access to RESTRICTED information or information that originates from the GSi*

4.4.5.4 All employees, *consultants, agency staff,* contractors and third party users who require IT access shall be required to agree to the terms and conditions of this policy and this will be formally recorded.

4.4.5.5 A formal disciplinary process for employees who have committed a security breach shall be in place.

4.4.6 During their term of office, Members shall apply security in accordance with established policies and procedures in relation to ICT and where relevant the Members Code of Conduct.

4.4.6.1 All Members who require computer access shall receive security awareness training as part of the formal induction process.

4.4.6.2 The security awareness training shall include legal responsibilities, business controls as well as training in the correct use of information processing facilities, e.g. logon procedures, use of software packages and information on the disciplinary procedure. *Additionally it will cover data handling and an awareness of how to handle personal data.*

DRAFT

4.4.6.3 All Members who require IT access shall be required to agree to the terms and conditions of this policy and this will be formally recorded.

4.4.6.4 If by breaching this security policy it results in a breach of the Members Code of Conduct they may be reported to the *Monitoring Officer* for investigation.

4.4.6.5 All Members shall return to the IT Training Officer all of the Council's assets in their possession upon standing down as a Member.

4.4.7 On termination or change of employment this process should be managed to ensure that all equipment is returned and the removal or change of all access rights are completed.

4.4.7.1 The IT Support Officer shall receive regular notification from HR of changes to the establishment.

4.4.7.2 The IT Support Officer shall receive notification from HR prior to the start date of additions to the establishment.

4.4.7.3 On receiving notification of change or termination of employment the IT Support Officer shall liaise with the relevant Head of Service to ensure that all Council information is retained appropriately and that the user logon is terminated.

4.4.7.4 All employees, contractors and third party users shall return, to their Head of Service, all of the Council's assets in their possession upon termination of their employment, contract or agreement.

4.4.7.5 Where passwords are known by an employee who is leaving and the account that the password relates to will remain active, the password shall be changed.

DRAFT

4.5 **Physical and environmental security**.
The objective is to prevent unauthorised physical access, damage and interference to the Council's premises and information.

4.5.1 Security perimeters should be used to protect areas that contain information and information processing facilities.

4.5.1.1 Access to non-public areas shall be controlled through appropriate physical access controls.

4.5.1.2 All Council buildings, where there is ICT equipment, shall be alarmed and, where appropriate, covered by CCTV cameras.

4.5.2 Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

4.5.2.1 Only designated staff are allowed unaccompanied access in the machine rooms.

4.5.2.2 Specific core keys for access to the machine rooms shall only be available to designated staff.

4.5.2.3 Third party support staff personnel may have restricted access to the machine rooms, this access shall be monitored.

4.5.3 Physical security for offices, rooms and facilities should be designed and applied.

4.5.3.1 All equipment shall be sited within the Council's premises so as to reduce the risks of damage, interference or unauthorised access.

4.5.4 Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster should be designed and applied.

4.5.4.1 Hazardous or combustible materials shall be stored at a safe distance from machine rooms.

4.5.4.2 Back-up media shall be stored at the Depot.

4.5.4.3 Appropriate fire fighting equipment shall be provided and suitably placed.

4.5.5 Physical protection and guidelines for working in secure areas should be designed and applied.

4.5.5.1 A procedure shall be in place as to how to operate the "nitrogeon" system in the machine rooms.

DRAFT

4.5.6 Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises should be controlled.

4.5.6.1 Incoming equipment shall be registered in accordance with the asset procedures as soon as the equipment is received.

4.5.7 Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

4.5.7.1 Information processing facilities handling sensitive data shall be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons.

4.5.7.2 Machine rooms shall be protected from power failures or other electrical anomalies.

4.5.7.3 Sherwood Lodge shall be protected from a loss of power by the standby generator.

4.5.7.4 Hardware at Leisure Centres shall be sited in lockable offices which must be locked when the office is unoccupied.

4.5.7.5 Hardware at Pleasley shall be sited in lockable offices which must be locked when the office is unoccupied.

4.5.8 Equipment should be correctly maintained to ensure its continued availability and integrity.

4.5.8.1 Equipment shall be maintained in accordance with manufacturer's instructions.

4.5.8.2 Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance.

4.5.9 Security should be applied to off-site equipment taking into account the different risks of working outside the Council's premises.

4.5.9.1 Equipment and media taken off the premises shall not be left unattended in public places.

4.5.9.2 Home working controls shall be specified within *any* mobile/remote working policy.

4.5.10 All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

DRAFT

4.5.10.1 All equipment shall have the storage media securely reformatted prior to disposal.

4.5.11 Equipment, information or software should not be taken off-site without prior authorisation.

4.5.11.1 Equipment that is temporarily taken off site shall be marked as such in the asset register.

4.5.11.2 Authorisation of home/mobile workers shall be at the discretion of Heads of Service.

4.5.11.3 Unless you have Council issued hardware or have previously been authorised to do so, no software or information shall be taken off site without obtaining the prior permission of the Head of ICT.

4.5.11.4 Spot checks of the location of assets may take place at any time.

4.5.11.5 *No information that contains customer, elected Member or employee details may be removed from the Council's premises unless there is a proven business need, in which case the information shall be encrypted.*

4.5.11.6 Where there is a business need to transfer customer, elected Member or employee information to a third party, the information shall be encrypted.

4.5.11.7 Those employees who take personal data off site on a memory stick may only do so on an encrypted memory stick issued by ICT. The employee is responsible for making ICT aware that this is required.

4.5.11.8 Those employees who hold personal data on the C: drive (hard disk) of a laptop, that is taken off site, may only do so if the hard disk has been encrypted by ICT. The employee is responsible for making ICT aware that this is required.

4.5.11.9 Those employees who send personal information via emails or emails attachments outside of the Council shall ensure that suitable encryption software is used. The employee is responsible for making ICT aware that this is required.

DRAFT

4.6 **Communications and operations management**
The objective is to ensure the correct and secure operation of information processing facilities, to minimise the risk of system failures and to protect against malicious and mobile code.

4.6.1 Operating procedures should be documented, maintained, and made available to all users who need them.

4.6.1.1 Documented operating procedures shall be held electronically on a knowledge base on the Help Desk server.

4.6.1.2 A paper copy of the documented operating procedures shall be held at the Depot.

4.6.1.3 Access to the documented operating procedures shall be limited to members of the ICT Service.

4.6.1.4 Responsibility for maintaining the documented operating procedures is with the *Senior 1st Line Support Officer.*

4.6.2 Changes to information processing facilities and systems should be controlled.

4.6.2.1 All changes to operating systems and application software shall be recorded in a formal change control log.

4.6.2.2 All changes shall be authorised by the Head of ICT Services prior to application.

4.6.2.3 A formal change control procedure shall be in place. *Details of this are available from the Senior 1st Line Support Officer*.

4.6.2.4 Responsibility for change control is with the *Senior 1st Line Support Officer.*

4.6.3 Development, test and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.

4.6.3.1 Rules for the transfer of software from development to operational status shall be defined and documented.[1]

4.6.3.2 Development and operational software shall run on different systems.

4.6.3.3 The test system environment shall emulate the operational system environment as closely as possible.

DRAFT

4.6.4 The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

4.6.4.1 Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

4.6.5 Acceptance criteria for new information systems, upgrades and new versions should be established and suitable tests of the systems carried out during development and prior to acceptance.

4.6.5.1 Performance and capacity requirements shall be assessed prior to acceptance.

4.6.5.2 Appropriate tests shall be carried out to ensure that all acceptance criteria have been fully satisfied.

4.6.5.3Training in the operation or use of new systems shall take place before acceptance.

4.6.5.4 The appropriate Head of Service shall authorise the live implementation after checking the testing log.

4.6.6 Detection, prevention and recovery controls to protect against malicious or mobile code and appropriate user awareness procedures should be implemented.

4.6.6.1Each P.C. and Server shall have anti-virus software installed

4.6.6.2The anti-virus software shall be regularly updated

4.6.6.3 A procedure shall be published on the intranet ensuring that all users are aware of the action to be taken if they suspect malicious code.

4.6.6.4 Business continuity plans shall be in place to recover from a virus attack.

4.6.6.5 Technical measures shall be activated as appropriate on specific systems to ensure mobile code is managed.

4.6.7 Backup copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

4.6.7.1 A backup policy shall be documented for internal use by ICT.

4.6.7.2 Backup copies of essential business data and software shall be regularly taken.

DRAFT

4.6.7.3 All backup media shall be stored off site as soon as possible.

4.6.7.4 Prior to removal off site the backup media shall remain in the machine rooms.

4.6.7.5 Backup media shall be regularly tested, *at least annually*, to ensure that they can be relied upon for emergency use when necessary.

4.6.8 Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

4.6.8.1 Access rights shall be applied to prevent unauthorised access to information.

4.6.8.2 Access rights shall be applied to prevent unauthorised access to applications.

4.6.8.3 Requests to access systems by third parties shall be authenticated and logged.

4.6.8.4 Remote access by staff and Members shall be authenticated.

4.6.8.5 A firewall shall be in place.

4.6.8.6 The associated firewall activity log should be monitored on a regular basis by the network and support officer.

4.6.8.7 Dial up access to the network is controlled by virtual private network technology *and two factor authentication*.

4.6.8.8 External audits of network security shall take place.

4.6.8.9 Performance of the network shall be pro-actively monitored by the network and support officer.

4.6.9 There should be procedures in place for the management of removable media. Removable media includes tapes, disks, memory sticks, removable hard drives, CDs, DVDs and printed media.

4.6.9.1 Removable media drives should only be enabled if there is a business reason for doing so.

4.6.9.2 All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications.

DRAFT

4.6.9.3 Any re-usable media that is no longer required, *in particular when an employee leaves,* shall be returned to the ICT Service where any information will be made unrecoverable.

4.6.9.4 Any media excluding printed media shall be returned to the ICT Service for secure disposal.

4.6.9.5 Printed media shall be disposed of in the paper shredding bins supplied to each Service in a timely manner.

4.6.9.6 Printed media, holding sensitive personal data, shall be shredded, in the dedicated facility provided, by the appropriate Service.

4.6.10 System documentation should be protected against unauthorised access.

4.6.10.1 System documentation shall be stored securely.

4.6.10.2 The access list for system documentation shall be restricted and authorised by the application owner.

4.6.11 Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

4.6.11.1 Anti-virus software shall be in place on the email server.

4.6.11.2 Instructions specifying the acceptable use of email shall be in place and available to all staff via the intranet.

4.6.11.3 Instructions specifying the acceptable use of internet access shall be in place and available to all staff via the intranet.

4.6.11.4 Sensitive information shall not be left on answering machines.

4.6.11.5 The courier system shall be used to protect information that is physically transferred between the Council's sites.

4.6.11.6 Instructions on CCTV are covered by the CCTV code of practice and standard operating procedures

4.6.12 Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

4.6.12.1 Authorisation processes shall be in place as to who may issue or sign key trading documents.

DRAFT

4.6.12.2 Electronic commerce arrangements shall be supported by a documented agreement.

4.6.12.3 The infrastructure for electronic commerce shall be subject to regular network penetration testing.

4.6.13 Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

4.6.13.1 Storage of any transaction details shall be behind the firewall and not directly accessible from the internet.

4.6.13.2 Authentication of customers shall be via *Government Gateway*

4.6.13.3 No information shall be published on the web site without prior approval of the Communications Officer.

4.6.13.4 The integrity of the Council's information on the web shall be protected to prevent unauthorised modification.

4.6.13.5 The infrastructure for on-line transactions shall be subject to regular network penetration testing.

4.6.14 Systems should be monitored and information security events should be recorded.

4.6.14.1 Audit logs recording information security events shall be maintained.

4.6.14.2 These audit logs may contain intrusive and confidential personal data, access will be limited to the Senior IT Projects Officer and Senior management on request.

4.6.14.3 Monitoring of internet use shall take place.

4.6.14.4 Monitoring of email use shall take place.

4.6.14.5 Periodic random monitoring of privileged operations shall take place.

4.6.14.6 Periodic monitoring of system alerts or failures shall take place.

4.6.14.7 *Periodic monitoring of PCs to check for such as illicit images will take place*

4.6.14.8 Clocks of all relevant information processing systems shall be synchronised with an agreed accurate time source.

DRAFT

4.7 **Access Control**
The objective is to control access to information, information processing facilities and business processes on the basis of business and security requirements and to prevent unauthorised access.

4.7.1 There should be a formal user registration and de-registration procedure.

4.7.1.1 Access to systems shall be controlled by business needs.

4.7.1.2 Each member of staff and elected Member with computer access shall have a unique logon id.

4.7.1.3 Users shall sign a statement to indicate that they understand the conditions of access.

4.7.1.4 *Staff who handle RESTRICTED information shall be required to sign a statement outlining the conditions of access to the GSi*

4.7.1.5 Service Heads shall ensure that access to systems is not allowed until the authorisation procedures have been completed.

4.7.1.6 A formal record shall be kept by ICT of all persons with authorised access.

4.7.1.7 Access shall be disabled when a member of staff leaves *unless a prior agreement has been made by the Head of Service*.

4.7.1.8 Change of duties shall cause a review of computer access required.

4.7.1.9 Staff suspended pending a disciplinary investigation shall have their access removed.

4.7.1.10 Periodic audits of access shall be undertaken by the IT Support Officer.

4.7.2 The allocation and use of privileges should be restricted and controlled.

4.7.2.1 Privileges shall be allocated on a need to use basis and on an event by event basis.

4.7.2.2 Privileges shall be assigned to a different user id from that used for normal business use.

4.7.2.3 A log of changes to database tables shall be kept by the privileged user and available to internal *and external* Audit *and any other organisations with approval*

DRAFT

4.7.2.4 A record of privileged users shall be kept detailing the tools they have access to on which systems.

4.7.3 The allocation of passwords should be controlled through a formal management process.

4.7.3.1 Users shall be required to maintain their own passwords.

4.7.3.2 Users shall initially be supplied with a secure temporary password which they are forced to change *the first time they access a system*.

4.7.3.3 A user must be verified before providing new, replacement or temporary passwords.

4.7.3.4 Users shall acknowledge receipt of passwords.

4.7.3.5 Passwords shall not be stored on computer systems in an unprotected form.

4.7.3.6 Default vendor passwords shall be altered following installation of systems or software.

4.7.3.7 Passwords shall not be written down with the exception of the ICT server and system passwords which shall be stored in the ICT password register.

4.7.3.8 The password register shall be kept in a locked place with restricted access.

4.7.3.9 Passwords shall not be disclosed.

4.7.3.10 Passwords shall be subject to periodic enforced change, generally 90 days.

4.7.4 Users should be required to follow good security practices in the selection and use of passwords.

4.7.4.1 Users shall change their password whenever there is any indication of possible system or password compromise.

4.7.4.2 Users shall select *sufficiently complex* passwords with sufficient minimum length, at least seven characters.

4.7.4.3 Passwords shall not be included in any automated logon process.

4.7.4.4 Users shall not use the same password for business and non-business use.

DRAFT

4.7.4.5 Users shall be locked out of systems after 3 unsuccessful login attempts.

4.7.5 Users should ensure that unattended equipment has appropriate protection.

4.7.5.1 Equipment must not be left logged in and unattended, *a PC screen must be locked when unattended.*

4.7.5.2 Users must logoff PCs when the session is finished (i.e. not just switch off the PC screen).

4.7.5.3 *PCs must be switched off, at the plug, at the end of the day*.

4.7.6 Appropriate authentication methods should be used to control access by remote users.

4.7.6.1 A solution shall be in place to encrypt and authenticate data to protect against eavesdropping and data tampering.

4.7.6.2 An VPN shall be in place to protect remote users requiring connection.

4.7.6.3. *Two factor authentication shall be in place for all remote users.*

4.7.7 Access to information and application system functions by users and support personnel should be restricted.

4.7.7.1 Menus shall be provided to control access to application system functions.

4.7.7.2 A log shall be maintained of all staff who have access to database editors.

4.7.7.3 A procedure shall be in place for changing data in database tables

4.7.8 When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied.

4.7.8.1 Remote access to business information across public network using mobile computing facilities shall only take place after successful identification and authentication.

4.7.8.2 Training shall be given to staff using mobile equipment to raise their awareness on the additional risks.

4.7.8.3 A home working policy shall be in place.

4.7.9 A regular audit shall take place by the Council's audit staff to confirm that all the controls within 4.7 are being adhered to.

DRAFT

4.8 **Information systems acquisition, development and maintenance**

The objective is to ensure that security is an integral part of information systems.

4.8.1 Specifications for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

4.8.2 All new systems must be advised to the Data Protection Officer.

4.8.3 New systems must be approved by the ICT Strategy Group prior to approval.

4.8.4 All systems purchased must have processes that validate data input and output.

4.8.5 All acquisitions, development and maintenance of systems must be done in a test area and documented testing done before transfer to the live system.

4.8.6 No software shall be installed unless it can be shown to have a valid licence.

4.8.7 No software shall be installed by anyone other than a member of the ICT staff.

4.8.8 A rollback strategy must be in place before changes are implemented.

4.8.9 Physical or logical access shall only be given to suppliers for support purposes when necessary, and with approval. The supplier's activities shall be monitored *and times of access documented*.

4.8.10 The use of operational databases containing personal or sensitive information for testing purposes shall be avoided.

4.8.11 Formal change control procedures shall be followed prior to the introduction of new systems and major changes to existing systems.

4.8.12 Proposed changes to operating systems shall be tested to ascertain impact on business systems.

4.8.13 Timely information about technical vulnerabilities of information systems being used shall be obtained, the Council's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

4.8.14 The acquisition of packaged software shall be subject to the approval of a business case by the IT Strategy Group.

DRAFT

4.8.15 Desktop software icons, for critical systems such as Housing Benefits, shall display the version number before the user activates the icon.

4.9 **Information security incident management**

The objective is to ensure information security events, possible security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. It is also to ensure that a consistent and effective approach is applied to the management of information security incidents.

4.9.1 All suspected security events and weaknesses shall be reported to the Senior IT Projects Officer. This shall be by either email, phone or in person.

4.9.2 Monitoring of email and internet use may also result in a security event being raised.

4.9.3 The Senior IT Projects Officer shall investigate the event or weakness as soon as feasibly possible.

4.9.4 If appropriate, the Senior IT Projects Officer shall inform the relevant Head of Service of a suspected event.

4.9.5 If the event involves customer or employee data the Senior IT Projects Officer will inform the Data Protection Officer.

4.9.6 Under no circumstances shall the individual reporting a weakness attempt to prove the weakness themselves, this could be interpreted as a misuse of the system.

4.9.7 A log shall be kept by the Senior IT Projects Officer of all suspected events and weaknesses with the results of the investigation.

4.9.8 On the conclusion of any security investigation, details are to be reported to the ICT strategy group and if appropriate the Head of Service and/or Head of HR for further action.

4.9.9 Information security incidents must be reported to *GovCertUk* and to the East Midlands WARP.

DRAFT

4.10 **Business Continuity Management**
The objective is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

4.10.1 A business continuity plan is in place.

4.10.2. The plan shall include reference to the IT disaster recovery plan.

4.10.3 The IT disaster recovery plan shall include identification of all responsibilities.

4.10.4 The IT disaster recovery plan shall identify the acceptable loss of information and services.

4.10.5 The IT disaster recovery plan shall include documentation of agreed procedures and processes.

4.10.6 The plans shall be reviewed regularly, at least annually.

4.10.7 The plans shall be tested regularly, at least annually.

4.11 **Compliance**
The objective is to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

4.11.1 Users are to comply with the following.

Computer Misuse Act 1990

The Computer Misuse Act 1990 makes it a criminal offence to access, or attempt to access, computer material. Persons convicted of an offence under the Computer Misuse Act are subject to a maximum of 5 years' imprisonment, a fine or both. In the context of Council users, it is likely that the following examples would be considered illegal:

- Accessing restricted material without proper Council.
- Provision of any material, such as codes or 'hacking' instructions which enables others to gain unauthorised access to a computer system.
- Knowingly receiving (or using) any material from an unauthorised user who has gained access to systems.
- Unauthorised modification of a computer system program or data stored on a system. (Includes the introduction of malicious software such as Viruses, Trojans, Worms, Spyware etc)
- Any material which encourages or incites other persons to carry out unauthorised access or modification of a computer system, program or data.

DRAFT

The Copyright Designs and Patents Act 1988

It is an offence under this Act to copy software or other Internet material without Council. It is immaterial whether such unauthorised copying is done with a view to persona convenience or for monetary gain. Unlimited fines and up to two years' imprisonment may be imposed on offenders.

All software, including commercial products and Shareware, is protected by copyright law and is licensed for legitimate use. Some software creators have designated their products Freeware (for which use is authorised without a licence fee being payable) and have made this available on the Internet. The Council does not tolerate the use of unauthorised/unlicensed software and permission is to be granted by the ICT Helpdesk before any software is loaded onto Council owned IT assets. No copies are to be made of software held by this Council unless clear guidance and permission is granted by the copyright holder

Data Protection Act 1998

This Act prohibits the holding, processing or disclosure of personal information data about others, unless the data user is properly registered and observes the data protection principles. Members and staff are to ensure they are conversant with the Council's and their Service's Data Protection Policy.

Age, Disabilities, Race Relations, Religious and Sexual Discrimination Acts

Discrimination on the grounds of race, age, gender disability, sexual identity, national origin, sexual orientation, religion or belief is unlawful under the provisions of the respective legislation. This covers private and public sectors and will include every member of the workforce, young and old. Any material published or received via the Internet (or by other means) which discriminates or encourages discrimination is in contravention of the legislation.

Regulation of Investigatory Powers Act (RIPA) 2000

RIPA prohibits the interception of e-mails without first obtaining the consent of both the sender and the recipient. However, the Regulations, which came into force on 2 October 2002, provide an important exception to the general rule that communications may only be monitored with consent.

The regulations enable businesses to intercept telecommunications (this includes telephone calls, and any data transmitted over the telecommunications network) without their employees consent for certain legitimate purposes, including detecting unauthorised use of

DRAFT

the system and ensuring its efficient operation. However, the employer must make reasonable efforts to inform employees that communications may be monitored.

The Human Rights Act 1998

Article 8 of the Human Rights Act states that *"everyone shall have the right to respect for his private and family life, his home and his correspondence".* However, this right is qualified and may be interfered with in order to protect the rights and freedoms of others. An employer, for example, may claim that, by monitoring e-mails, it is protecting the rights of other employees to have a workplace which is free of discrimination (assuming the employer prohibits the sending of discriminatory material via e-mail). Similarly, the employer may legitimately argue that, by having CCTV, it is providing its employees with a safe work environment and further, taking action which is necessary to prevent crime.

Criminal Justice and Public Order Act 1994

This miscellany of legislation includes a consolidation of provisions for the protection of minors by making it a criminal offence to possess pornographic or obscene material of or involving minors or material considered to be excessively violent. In the context of the Internet it would apply to the transmission, receipt and storage of text, audio and graphic images.

Laws of Defamation

Any publication of a statement, comment or innuendo about another individual or Council which cannot be justified at law may render the author liable to an action of defamation. In the context of Internet use, the Council will not permit the publication of defamatory material and any author transmitting or any person passing on defamatory material will be required to indemnify the Council against all actions, proceedings, claims and costs resulting there from.

Obscene publications Act 1959

The publication (whether for gain or not) of material intended to be read, heard or looked at which is as to tend to deprave and corrupt persons having access to the publication is a criminal offence which carries a maximum sentence of three years' imprisonment.

Telecommunications *(Fraud) Act 1997*

A person who sends a message or other matter that is grossly offensive, indecent, obscene or menacing in character via the public telecommunication system or sends a false message for the

DRAFT

purpose of causing annoyance, inconvenience or needless anxiety to another shall be guilty of a criminal offence. Email/Internet makes use of the "public telecommunication system". A breach of this Act will result in a substantial fine and/or imprisonment.

Freedom of Information Act,

Guidelines on this act can be found on intranet. Any requests for information under this act must be dealt with in accordance with Council Policy.

CCTV code of Practice 2008

This is published by the Information Commisioner.

Bolsover District Council Financial Regulations

Specific elements of these regulations which apply are:

- Security – Section 4.7.15.
- Council Assets – Section 4.7.17.
- *Fraud, Corruption and* Irregularities – Section 4.7.20.
- Information Technology – Section 4.7.23.
- Retention of Financial Records – Section 4.7.24.

4.11.2 Anyone found breaching these regulations will face disciplinary action, which may result in dismissal, suspension or investigation by the Police.

4.11.3 Access to ICT auditing systems will be limited to authorised ICT personnel and Auditors.

4.11.4 Employees and elected Members should be aware of the following guidance on the Intranet:

- Access to Information Policy
- Whistle Blowers Charter
- Email and Internet (use of) Policy
- CCTV Codes of Practice

5. Responsibility for implementing the Policy

Responsibility for implementing this Policy is with the Head of ICT.

DRAFT

6.Glossary of terms

Term used	Definition
Asset	Anything that has value to the Council.
GSi	*Government Secure Intranet is a system for managing secure access to e-mail and other services for UK government departments*
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information	Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on film, or spoken. Whatever form the information takes, or means by which it is shared or stored, appropriate measures must be in place to ensure that this information is protected.
Restricted	*Restricted information is defined as any asset whose compromise would be likely to:* ▪ *Adversely affect diplomatic relations* ▪ *Cause substantial distress to individuals* ▪ *Make it more difficult to maintain the operational effectiveness or security of UK or allied forces* ▪ *Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies* ▪ *Prejudice the investigation or facilitate the commission of crime* ▪ *Breach proper undertakings to maintain the confidence of information provided by third parties* ▪ *Impede the effective development or operation of government policies* ▪ *Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and/or the e-government security framework)* ▪ *Disadvantage government in commercial or policy negotiations with others* ▪ *Undermine the proper management of the public sector and its operations*

DRAFT

Term used	Definition
VPN	A Virtual Private Network, *as the Council uses it, is a computer network where the links between nodes are carried by a virtual circuit, the Internet, instead of by physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. This functionality gives us secure comunication links.*
WARP	A **W**arning, **A**dvice and **R**eporting **P**oint for computer security incidents. Usually run regionally.
Personal information	*The difference between personal and personal sensitive information is that personal sensitive data relates to areas such as an individual's racial origin, religious beliefs, physical/mental health, political beliefs etc. For the purpose of this policy the definition of personal information includes both personal and personal sensitive information.*
Two factor authentication	*This is a system wherein two different factors are used in conjunction to authenticate users. Using two factors as opposed to one factor delivers a higher level of authentication assurance. Generally it is something that you have and something that you know.*
Information Asset Owner	*A business manager who operationally owns the information contained in their systems. Their role is to understand what information is held, how it is used and transferred, and who has access to it and why, in order for business to be transacted within an acceptable level of risk. They regularly review user access rights.*
Rollback strategy	A strategy decided before a change happens so that in the event of a change failing or having an unexpected result, the database or group of records can be returned to the state prior to the change.

DRAFT