East Northamptonshire Council

Personnel Sub Committee - 31 August 2010

Information Security Policy

Summary

To seek adoption of the Information Security Policy

Attachment(s)

Information Security Policy

1.0 Background

1.1 Information is a key business asset and fundamental to the delivery of public services. Like any other key business asset it must be suitably protected.

1.2 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. It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level which is appropriate to the Council's needs.

1.3 The Information Security Policy is actually a collection of fourteen policies which are based on industry good practice and have been developed to satisfy the requirements set out by the Government Connect Secure Extranet Code of Connection (CoCo) and the Data Protection Act.

2.0 Protecting information

2.1 Protecting information relies on people, processes and technology. The Council needs a culture that values and protects information and requires the appropriate policies, procedures and technology to be in place.

2.2 Whilst some of the policies just confirm what we do already there are some that require us to adopt different ways of working.

2.3 Once the Information Security Policy has been adopted by the Council the rollout will need to ensure all staff are not only aware of the policies but understand their responsibilities under each policy. Also the appropriate processes and technology will need to be in place.

2.4 Adhering to the Information Security Policy will significantly reduce the risk of information security incidents, and in doing so, will help us build the necessary public trust in the handling of personal information.

3.0 Adoption of Policy

3.1 Staff have been consulted on the Information Security Policy via the XChange Group.

3.2 We recognise that changing the data handling culture will be the biggest challenge and that there is a lot of work to do before the Information Security Policy is embedded into the organisation.

4.0 Recommendation

4.1 It is recommend that the Policy is adopted by the Council so that this work can begin.

Implications:			
Corporate Outcomes or Other Policy/Priority/Strategy			
Good Quality of Life	☐	Good Reputation	☒
Good Value for Money	☐	High Quality Service Delivery	☒
Effective Partnership Working	☒	Strong Community Leadership	☐
Effective Management	☒	Knowledge of our Customers and Communities	☐
Employees and Members with the Right Knowledge, Skills and Behaviours			☒
Other:			☐
Decision(s) would be outside the budget or policy framework and require full Council approval			☐
Financial	There are no financial implications at this stage		☒
	There will be financial implications – see paragraph		☐
	There is provision within existing budget		☐
	Decisions may give rise to additional expenditure at a later date		☐
	Decisions may have potential for income generation		☐
Risk Management	An assessment has been carried out and there are no material risks		☒
	Material risks exist and these are recorded at Risk Register Reference - inherent risk score - residual risk score -		☐
Staff	There are no additional staffing implications		☒
	Additional staff will be required – see paragraph		☐
Equalities and Human Rights	There will be no impact on equality (race, age, gender, disability, religion/belief, sexual orientation) or human rights implications		☒
	There will be an impact on equality (see categories above) or human rights implications – see paragraph		☐
Legal	Power:		
	Other considerations:		
Background Papers:			
Person Originating Report: Gareth Jones, Head of ICT Services, 01832 742076			
Date: 10 August 2010			

CFO		**MO**		**CX**	

(Committee Report Normal Rev. 21)

East Northamptonshire Council

Borough Council of Wellingborough

Information Security Policy

Protecting our information

Document Version Control

Author (Post holder title)	Information Governance & Programme Manager
Type of document (strategy/policy/procedure)	ICT Policy
Version Number	0.4
Document File Name	J:\ICT\Policies\ Information Security Policy
Issue date	August 2010
Approval date and by who (SMT / committee)	
Document held by (name/section)	
For internal publication only or external also?	Unclassified
Next review date	August 2013

Change History

Issue	Date	Comments
0.1	January 2010	Localised for East Northamptonshire Council
0.2	April 2010	New corporate format
0.3	June 2010	Amalgamated all the information security policies and distinguished between Council business and Councillor business
0.4	August 2010	Incorporated comments from Xchange. Removed all references to Councillors

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
Employees	

Distribution List

Internal	External
Employees	

Links to other documents

Document	Link
Information and Records Management Policy	
Local Government Retention Guidelines	

Additional Comments to note

Contents

1.0 Introduction

1.1 This policy incorporates a number of information security policies adopted by East Northamptonshire Council and the Borough Council of Wellingborough. These information security policies have been developed to ensure that high confidentiality, integrity and availability standards of information are maintained at both Councils.

1.2 The Councils depend on information, including personal information, to carry out their business effectively, and it is the responsibility of all Council employees to ensure that this information is handled appropriately.

1.3 The information that the Councils hold, process, maintain and share with other public sector organisations is an important asset that, like any other important business asset, needs to suitably protected.

1.4 The information needs to be protected so that it is:

- only accessible to those authorised to have access;
- not changed in any unauthorised way; and
- available when needed

1.5 This means keeping it stored securely, whatever form it is in, thinking carefully about the benefits and risks of sharing it with others and, when it is no longer required, destroying it properly.

1.6 The Data Protection Act 1998 requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage.

2.0 Scope

2.1 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. It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Council's needs.

2.2 The objective of these policies is to ensure the highest standards of information security are maintained across the Councils at all times so that:

- The public and all users of the Council's information systems are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by information security incidents are minimised.
- All legislative and regulatory requirements are met.
- The Council's ICT equipment and facilities are used responsibly, securely and with integrity at all times.

2.3 The information security policies contained within this policy are based on industry good practice and intend to satisfy the requirements set out by the Government

Connect Secure Extranet Code of Connection (CoCo) and the Data Protection Act. The policies are

- Email Acceptable Use Policy.
- Internet Acceptable Use Policy.
- Software Policy.
- IT Access Policy.
- Information Protection Policy.
- Computer, Telephone and Desk Use Policy.
- Legal Responsibilities Policy.
- Information Security Incident Management Policy.
- Removable Media Policy
- Remote Working Policy
- IT Infrastructure Security Policy
- User Information Security Standards Policy
- GCSx Acceptable Use Policy
- Communications and Operation Management Policy.

2.4 These policies apply to both East Northamptonshire Council and the Borough Council of Wellingborough. They are jointly referred to as "the Council".

2.5 These policies apply to all Council employees and any contractual third parties of the Council using the Council's ICT resources. These policies do not apply to Councillors.

3.0 Policy outcomes

3.1 The outcomes to be delivered by this policy are:

Information Security Policy outcomes	Links to corporate outcomes (delete as appropriate)
• Improved efficiency and effectiveness of service delivery and decision making	• A good reputation with customers and regulators • Effective management

4.0 Applying the Policy

4.1 Protecting information relies on people, processes and technology. The Councils need a culture that values and protects information and have the policies and technology in place to support this.

4.2 As part of this culture all employees that handle personal information will be expected to undertake appropriate training.

4.3 All users have a responsibility to protect the information they handle and are required to read, understand, and adhere to all the Council's information security policies that are appropriate for their role. A copy of the Information Security Policy Acceptance form is available in Appendix 1. Non-compliance with the policies may result in disciplinary action.

4.4 Extra controls need to be applied to protect information that is classed as PROTECT or RESTRICTED (see Information Protection Policy Appendix) and the different policies address these.

4.5 Users should also understand the relevant legislation relating to Information Security and be aware of their responsibilities under this legislation. The legislation covers:

- The Freedom of Information Act 2000.
- The Human Rights Act 1998.
- The Privacy and Electronic Communications Act 2003.
- The Regulation of Investigatory Powers Act 2000.
- The Data Protection Act 1998.
- The Copyright Designs and Patents Act 1988.
- The Computer Misuse Act 1990.
- The Environmental Information Regulations 2004.

Users can be held personally and legally responsible for breaching the provisions of the above Acts.

1 Email Acceptable Use Policy

1.1 Scope

1.1.1 This policy covers all email systems and facilities that are provided by the Council for the purpose of conducting and supporting official Council business through the Council's network infrastructure and all standalone and portable computer devices.

1.1.2 All email prepared and sent from Council email accounts, and any non-work email sent using Council computer equipment, is subject to this policy.

1.1.3 This policy aims to mitigate the following risks:

- Disclosure of PROTECT and RESTRICTED information as a consequence of incorrect use of email.
- Contamination of Council networks or equipment through the introduction of viruses through the use of email.
- Potential legal action against the Council or individuals as a result of the illegal use of email.
- Reputational damage to the Council as a result of misuse of email.

1.2 Applying the Email Acceptable Use Policy

1.2.1 Email as Records

1.2.1.1 All emails that are used to conduct or support official Council business **must** be sent using an "@east-northamptonshire.gov.uk" or @wellingborough.gov.uk email account as appropriate. Non-work email accounts **must not** be used to conduct or support official Council business unless the Council's email system is unavailable.

1.2.1.2 All emails, including attachments that are used to conduct or support Council business may need to be disclosed under the Data Protection Act, the Freedom of Information Act, or Environmental Information Regulations therefore all such emails must be stored within the Council's network.

1.2.1.3 Users should refer to the Information and Records Management Policy for guidance on the keeping, management and destruction of their email records.

1.2.1.4 The legal status of an email message is similar to any other form of written communication. Consequently, any email message sent from equipment provided to conduct or support official Council business should be considered to be an official communication from the Council. All official outgoing external email **must** carry the Council's disclaimer. This is automatically applied when an external email is sent using the Council's email system.

1.2.1.5 Whilst respecting the privacy of authorised users, the Council 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.

1.2.1.6 Users should be aware that deletion of email from individual email accounts does not necessarily result in permanent deletion from the Council's ICT systems.

1.2.2 Email as a Form of Communication

1.2.2.1 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 this is the most appropriate method of communication in the particular circumstances.

1.2.2.2 All emails sent to conduct or support official Council business **must** comply with the Council's corporate communications standards.

1.2.2.3 Email **must not** be considered to be any less formal than memos or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to include any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.

1.2.2.4 Computer facilities provided by the Council for email **must not** be used for:

- the transmission of material such that this infringes the copyright of another person, including intellectual property rights;
- activities that unnecessarily waste the Council's ICT resources;
- activities that corrupt or destroy other users' data;
- the creation or transmission of any offensive, obscene or indecent images, data, or other material;
- the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others;
- the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, age, disability, political or religious beliefs;
- the creation or transmission of defamatory material;
- the creation or transmission of material that includes false claims of a deceptive nature;
- so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms;
- activities that violate the privacy of other users;
- unfairly criticising individuals, including copy distribution to other individuals;
- the creation or transmission of material which brings the Council into disrepute.

1.2.3 Junk Email

1.2.3.1 There may be instances where a user will receive unsolicited mass junk email or spam. Users should immediately delete any unwanted email messages and unsubscribe from any unnecessary mailing lists.

1.2.3.2 Before giving their Council email address to a third party, for instance a website, users should 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.

1.2.3.3 Chain letter emails (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 the Council's systems or facilities.

1.2.4 Managing Emails

1.2.4.1 Users should avoid sending unnecessary messages in order not to overload the email system. In particular, the use of the Council wide email distribution list should only be used to communicate an urgent message, i.e. received within 24 hours, and the message affects everyone.

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

1.2.4.3 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 whenever possible rather than a copy of the file.

1.2.4.4 Users should refer to the guidance notes on Managing Emails for further advice.

1.2.4.5 Users should raise any concerns they may have, with using email or any particular emails that they find offensive, with the ICT Service Desk.

1.2.5 Monitoring of Email Usage

1.2.5.1 All users should be aware that email usage is monitored and recorded by ICT Services. The monitoring of email (outgoing and incoming) traffic will be undertaken so that the Council:

- 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.

1.2.5.2 Monitoring of content will only be undertaken by ICT Services staff specifically authorised for that task with the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.

1.2.5.3 Any suspected misuse of email by employees should be reported to their manager. Designated staff in ICT Services can investigate and provide evidence and audit trails of access to systems. ICT Services will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

1.2.5.4 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 manager for specific work purposes whilst they are absent. If this is the case a request should be made to the ICT Service Desk. 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.

1.2.5.5 Use of generic email addresses, e.g. elections@east-northamptonshire.gov.uk for services should be encouraged rather than individual email addresses.

1.2.6 Classification of Emails

1.2.6.1 When creating an email, users **must** assess and classify the information contained within it in accordance with the Council's Information Protection Policy.

1.2.6.2 Senders **must** include the classification in the Subject line of any emails containing PROTECT or RESTRICTED information.

1.2.7 Security of Emails

1.2.7.1 Users **must** make every effort to ensure that the confidentiality of email is appropriately maintained. Users should take care when addressing emails to prevent accidental transmission to unintended recipients.

1.2.7.2 Emails sent between east-northamptonshire.gov.uk email accounts are held with the same network and are deemed to be secure. This also applies to emails sent between wellingborough.gov.uk addresses. However, emails which 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.

1.2.7.3 GCSx (Government Connect Secure Extranet) is a secure private network which enables secure emails to be sent between local authorities and organisations that sit on the pan-government secure network infrastructure. Therefore any emails containing PROTECT and RESTRICTED material which are to be sent outside of the Council's secure network **must** be sent via GCSx mail.

1.2.7.4 Data sent or received via GCSx mail should be stored separately to non-classified data.

1.2.7.5 Any users requiring access to GCSx email should contact the ICT Service Desk.

1.2.8 Negligent Virus Transmission

1.2.8.1 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 ICT Service Desk.

1.2.8.2 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 Council facilities.
- **Must not** forward virus warnings other than to the ICT Service Desk.
- **Must** report any suspected files to the ICT Service Desk.

1.2.8.3 In addition, ICT Services will ensure that email is virus checked before it enters the Council network and before it is stored on the server.

1.2.8.4 If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted.

2 Internet Acceptable Use Policy

2.1 Scope

2.1.1 This policy should be applied at all times whenever using the Council provided Internet facilities or using the Council's ICT equipment to access the Internet. This includes access via any Internet enabled device.

2.1.2 This policy aims to mitigate the following risks:

- Contamination of Council networks or equipment through the introduction of viruses through the downloading of unsuitable material from the Internet.
- Potential legal action against the Council or individuals as a result of accessing unsuitable material from the Internet.
- Reputational damage to the Council as a result of Internet misuse on Council equipment.

2.2 Applying the Internet Acceptable Use Policy

The Internet service is primarily provided to give Council employees:

- Access to information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained web sites.
- An electronic commerce facility.

2.2.1 Personal Use of the Council's Internet Service

2.2.1.1 Provided it does not interfere with work, the Council permits personal use of the Internet in the user's own time, e.g. before work, in their lunch-break, after work.

2.2.1.2 The Council is not however responsible for any personal transactions users enter into - for example in respect of the quality, delivery or loss of items ordered. Users **must** accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from their transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

2.2.1.3 If a user purchases personal goods or services via the Council's Internet service they are responsible for ensuring that the information they provide shows that the transaction is being entered into by them personally and not on behalf of the Council.

2.2.1.4 Users should ensure that personal goods and services purchased are not delivered to Council property. Rather, they should be delivered to their home or other personal address.

2.2.1.5 If a user is in any doubt about how they may make personal use of the Council's Internet Service they are advised not to do so or contact the ICT Service Desk.

2.2.1.6 All personal usage **must** be in accordance with this policy. ICT equipment provided by the Council and any data held on it are the property of the Council and may be

accessed at any time by ICT Services to ensure compliance with all the Council's statutory, regulatory and internal policy requirements.

2.2.2 Internet Account Management, Security and Monitoring

2.2.2.1 Internet access is recorded against the user's login (user id and password).

2.2.2.2 The provision of Internet access is owned by the Council and all access is recorded, logged and maybe interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.
- Ensuring that use of the Internet facility is relevant and appropriate to the Council's business and within the context of the user's role.

2.2.2.3 The filtering system monitors and records all Internet access for reports that can be produced for managers and auditors if appropriate.

2.2.3 Things Users Must Not Do

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

- Create, download, upload, display or access knowingly, unsuitable material i.e. is discriminatory, defamatory, harassing, obscene or pornographic.
- Infringe copyright agreements

"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 Council policies.

2.2.3.2 Users **must not**, under any circumstances, use their Internet account, to

- Subscribe to, enter or use online gaming or betting sites.
- Run a private business.
- Download any software that does not comply with the Council's Software Policy.

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

- Auctions
- Dating
- Drugs
- Gambling
- Gaming
- Hacking
- Hate & Discrimination
- Illegal
- Image Sites
- Instant Messaging
- Internet Telephony
- Military

- Newsgroups & Forums
- Offensive & Tasteless
- Peer to Peer
- Pornographic & Adult Material
- Proxy Avoidance
- SMS & Mobile Telephony Services
- Sex Education
- Software Download
- Streaming Media & Media Downloads
- Violence
- Weapons
- Webchat
- Weblogs & Social Interaction
- Webmail

If a user needs to access a website that is blocked they should contact the ICT Service Desk.

2.2.4 Users Responsibilities

2.2.4.1 It is the responsibility of users to understand and adhere to this policy. Users should contact the ICT Service Desk if they have any concerns regarding using the Internet.

2.2.4.2 Any suspected misuse of the Internet by Council employees should be reported to their manager.

2.2.5 Managers Responsibilities

2.2.5.1 It is the responsibility of managers to ensure that the use of the Internet facility within an employee's work time is relevant and appropriate to the Council's business and within the context of the employee's role.

3 Software Policy

3.1 Scope

3.1.1 This policy applies at all times when the Council's computer equipment is used.

3.1.2 This policy aims to mitigate the following risks:

- Contamination of Council networks or equipment through the introduction of viruses through the use of personal or unlicensed software.
- Potential legal action against the Council or individuals as a result of using illegal software.
- Reputational damage to the Council as a result of the use of illegal software on its equipment.

3.2 Applying the Software Policy

3.2.1 All software applications acquired by the Council **must** meet a business need, align with the Council's ICT Strategy and be purchased through ICT Services.

3.2.2 All software applications used by the Council **must** be licenced unless a licence is not required. The Council will not condone the use of any unlicensed software application.

3.2.3 The ICT Service Desk will maintain a register of all Council software applications and license details.

3.2.4 System Administrators **must** ensure software applications are only used in accordance with the license agreement.

3.2.5 Software applications, including free or evaluation software applications, must only be installed by ICT Services. Once installed, the original media will be kept in a safe storage area maintained by the ICT Service Desk.

3.2.6 Personal or unlicensed software **must** not be loaded onto the Council's computer equipment as there is a serious risk of introducing a virus, and/or committing a criminal offence.

3.2.7 The creation of digital databases, using Microsoft Access, outside of ICT Services is not permitted.

3.2.8 Illegal reproduction of software is subject to civil damages and criminal penalties as covered by the Copyright, Designs and Patents Act 1988. The Council does not condone the illegal duplication of software and will not tolerate it. Any Council employee or Councillor who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate.

3.2.9 Any suspected misuse of software by Council employees should be reported to their manager.

4 IT Access Policy

4.1 Scope

4.1.1 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.

4.1.2 Access control rules and procedures **must** be adhered to in order to control who can access the Council's information systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Council information systems in any format, and on any device.

4.2 Applying the IT Access Policy

4.2.1 Choosing Passwords

4.2.1.1 Computer passwords are an important part of ICT security and users have an essential role in protecting the ICT environment in which we work. Complex, unpredictable passwords help to ensure that non-authorised people do not misuse the network resources or compromise the security of our network and data.

4.2.1.2 A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. 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.

4.2.1.3 A strong password must be at least eight characters long and include at least three of the following four elements:

- lower case alpha characters
- upper case alpha characters
- numbers
- special characters

4.2.1.4 Users **must** choose strong passwords.

4.2.2 Protecting Passwords

4.2.2.1 It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the guidance notes on Passwords.
- Ensuring that any PC or laptop they are using is locked or logged out when left unattended.
- Not sharing their password with, or disclosing it to, anyone else.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Contacting the ICT Service Desk if they have any concerns or queries regarding passwords.

4.2.2.2 Users will be held responsible for all activities logged to their unique user login, i.e. user ID and password.

4.2.2.3 Users will be prompted to change their network password every 60 days. A history will be kept of the previous 20 successful passwords used. These passwords cannot be reused whilst they remain in the history.

4.2.2.4 System Administrators **must** ensure their systems will prompt users to change their system passwords regularly.

4.2.2.5 Users **must** immediately change any default passwords.

4.2.2.6 If a user becomes aware, or suspects, that their password has become known to someone else, they **must** change it immediately and report their concern to the ICT Service Desk.

4.2.2.7 Users should refer to the guidance notes on Passwords for further advice on creating a Strong Password and protecting their Passwords.

4.2.3 User Access Management

4.2.3.1 ICT Services will maintain procedures to ensure authorised user access and to prevent unauthorised access to information systems.

4.2.3.2 System Administrators will ensure each user

- is allocated access rights and permissions to information systems that are commensurate with the tasks they are expected to perform;
- has a unique user ID; and
- has an associated unique password that is requested at each new login.

4.2.4 Managers Responsibilities

4.2.4.1 Managers are responsible for submitting an IT Access Form to the ICT Service Desk for a new user, to change a user's access details, to suspend a user, or to remove a user. Any delay with this could result in an information security incident.

4.2.5 Partner agencies or 3rd Party Suppliers access

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

4.2.5.2 Partner agencies or 3rd party suppliers **must** contact the ICT Service Desk before connecting to the Council's network and a log of activity **must** be maintained. Remote access software **must** be disabled when not in use.

4.2.6 ICT Services Responsibilities

4.2.6.1 ICT Services will control access to operating systems by a secure login process. This process will:

- Not display any previous login information e.g. username.
- Limit the number of unsuccessful attempts and locking the account if exceeded.
- Hide the password characters with symbols.

4.2.6.2 ICT Services will provide users with access to the Council's network via a unique user ID that will be audited and can be traced back to the user. The user ID **must not** give any indication of the level of access that it provides to the system (e.g. administration rights).

4.2.6.3 ICT Services will ensure that users are not allowed to reuse the same password within 20 password changes.

4.2.6.4 ICT Services will provide System Administration accounts only to users that are required to perform system administration tasks.

4.2.7 System Administrator responsibilities

4.2.7.1 System Administrators **must not** use the system administrator account for normal day to day activities.

4.2.7.2 System Administrators of the software applications are responsible for granting access to the information within the system. The access **must**:

- be compliant with the User Access Management (see 4.2.3).
- be separated into clearly defined roles.
- give the appropriate level of access required for the role of the user.
- be unable to be overridden (with the admin settings removed or hidden from the user).
- be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- be logged and auditable.

4.2.7.3 System Administrators will review system access rights for all users annually to ensure that the appropriate rights are still allocated.

5 Information Protection Policy

5.1 Scope

5.1.1 This policy should be applied whenever Council information systems or Council information is accessed. 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 or video.
- Speech.

5.1.2 This policy aims to mitigate the following risks:

- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of a failure to protect its information assets.
- Potential legal action against the Council or individuals as a failure to protect its information assets.
- Reputational damage to the Council for failing to protect its information assets.

5.2 Applying the Information Protection Policy

5.2.1 Identifying Information Assets and Information Asset Owners

5.2.1.1 ICT Services and information asset owners will draw up and maintain an inventory of all important information assets that the Council relies upon.

5.2.1.2 For documents that have a specific, short term localised use, the creator of the document will be the information asset owner. This includes letters, spreadsheets and reports created by staff. The sender of an email is the owner of the information contained within the email.

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

5.2.2 Classifying Information Assets

5.2.2.1 Protective Marking System Criteria has been developed for use within the Council. This is to complement the Government Protective Marking System Criteria which is part of the HMG Security Policy Framework.

5.2.2.2 All information assets **must** be assessed and classified by the information asset owner in accordance with the Council's Protective Marking System Criteria (see Appendix).

5.2.2.3 Care **must** be taken to apply the correct level of classification and where possible information of different classifications should be separated. The classification will determine how the document should be protected and who should be allowed access to it.

5.2.2.4 The sensitivity of an information asset may change over time and it may be necessary to re-classify information assets. The information asset owner is responsible for re-classifying and re-marking information assets.

5.2.3 Marking Information Assets

4.3.1 PROTECT or RESTRICTED information **must** be clearly marked with the classification and it should be included in the folder or document name or email subject line. This is the responsibility of the information asset owner.

5.2.4 Disclosing PROTECT or RESTRICTED non-personal information

5.2.4.1 PROTECT or RESTRICTED non-personal information **must not** be disclosed to any other person or organisation before the information asset owner is consulted and advice sought from the Council's Monitoring Officer to establish whether the information can be disclosed. The information asset owner **must** ensure the information is unclassified and re-marked before the information is disclosed.

5.2.4.2 The restrictions on sending PROTECT or RESTRICTED information by email are covered in the Council's Email Acceptable Use Policy.

5.2.5 Sharing of Personal Information

5.2.5.1 This is covered in the Council's Legal Responsibilities Policy.

5.2.6 Disposing of Information Assets

5.2.6.1 Information asset owners should delete or destroy information if there is no legal or operational need to keep it. For guidance on retention periods of documents information asset owners should refer to the Retention Guidelines for Local Authorities.

5.2.6.2 All paper PROTECT and RESTRICTED documents **must** be disposed of as confidential paper waste.

Appendix - Government Protective Marking System Criteria

The criteria below provide a broad indication of the type of material at each level of protective marking in accordance with the HMG Security Policy Framework.

Criteria for assessing **TOP SECRET** assets:

- threaten directly the internal stability of the United Kingdom or friendly countries;
- lead directly to widespread loss of life;
- cause exceptionally grave damage to the effectiveness or security of United Kingdom or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations;
- cause exceptionally grave damage to relations with friendly governments;
- cause severe long-term damage to the United Kingdom economy.

Criteria for assessing **SECRET** assets:

- raise international tension;
- to damage seriously relations with friendly governments;
- threaten life directly, or seriously prejudice public order, or individual security or liberty;
- cause serious damage to the operational effectiveness or security of United Kingdom or allied forces or the continuing effectiveness of highly valuable security or intelligence operations;
- cause substantial material damage to national finances or economic and commercial interests.

Criteria for assessing **CONFIDENTIAL** assets:

- materially damage diplomatic relations (i.e. cause formal protest or other sanction);
- prejudice individual security or liberty;
- cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations;
- work substantially against national finances or economic and commercial interests;
- substantially to undermine the financial viability of major organisations;
- impede the investigation or facilitate the commission of serious crime;
- impede seriously the development or operation of major government policies;
- shut down or otherwise substantially disrupt significant national operations.

Criteria for assessing **RESTRICTED** assets:

- affect diplomatic relations adversely;
- cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces;
- cause financial loss or loss of earning potential or to 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;
- to breach statutory restrictions on disclosure of information;
- disadvantage government in commercial or policy negotiations with others;
- undermine the proper management of the public sector and its operations.

Criteria for assessing **PROTECT** (Sub-national security marking) assets:

- cause distress to individuals;

- breach proper undertakings to maintain the confidence of information provided by third parties;
- breach statutory restrictions on the disclosure of information;
- cause financial loss or loss of earning potential, or to facilitate improper gain;
- unfair advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- disadvantage government in commercial or policy negotiations with others.

Appendix - The Council's Protective Marking System Criteria

To complement the Government's Protective Marking System Criteria the Council will adopt the following classification guidelines

RESTRICTED

- Information marked as RESTRICTED
- Information that is highly sensitive and only available to specific, named individuals (or specific positions)
- Sensitive personal information (see the Legal Responsibilities Policy)
- Committee 'Pink Papers'
- Information provided in confidence

PROTECT

- Information marked as PROTECT
- Information that is sensitive outside the Council
- Personal information not in the public domain
- Authorised access to this information on a "need-to-know" basis for business-related purposes

unclassified

- Information not marked as PROTECT or RESTRICTED
- Information that could be available to anyone

6 Computer, Telephone and Desk use Policy

6.1 Scope

6.1.1 This policy should be applied whenever users use the Council's computer and telephony resources to access information systems or use Council information.

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

- Network facilities
- Personal computers
- Portable laptop computers, notebooks, tablets
- Cameras, MP3 players
- Printers
- Storage devices
- Blackberries, mobile phones

6.1.3 This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to PROTECT and RESTRICTED information.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

6.2 Applying the Computer, Telephone and Desk use Policy

6.2.1 Computer Resources Misuse

6.2.1.1 All users **must** adhere to the Computer Misuse Act which prohibits

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences; and
- Unauthorised modification of computer material.

6.2.1.2 All users **must** read and abide by all the Council's relevant information security policies.

6.2.2 Use of Computer and Telephone Equipment.

6.2.2.1 ICT Services will provide ICT equipment to meet a business need, where practicable.

6.2.2.2 Users are responsible for taking care of their Council supplied ICT equipment and for using it for the purpose for which it was supplied.

6.2.2.3 Users are responsible for reporting any problems with Council supplied ICT equipment to the ICT Service Desk.

6.2.2.4 Managers are responsible for reviewing the guidelines concerning the provision and personal use of Council's ICT equipment. Once approved, all users will be expected to adhere to these guidelines.

6.2.3 Clear Desk

6.2.3.1 A clear desk policy helps ensure that all information is held securely at all times. There may be a business requirement for someone other than the user to use the desk and computer.

6.2.3.2 Users **must** ensure that PROTECT or RESTRICTED information is secure when they are away from their desks.

6.2.3.3 Users **must** ensure that their computers are locked, when unattended, to prevent unauthorisd access.

6.2.3.4 At the end of each day PROTECT or RESTRICTED information **must** be locked away. Unclassified material may be left on desks.

6.2.3.5 Nothing should be left lying on printers, photocopiers or fax machines at the end of the day. Documents should be collected once printed.

6.2.4 Moving of ICT equipment

6.2.4.1 The ICT Support Team is responsible for moving all Council owned ICT equipment on Council premises. If a user needs their ICT equipment moving they must contact the ICT Service Desk.

6.2.4.2 The ICT Support Team is responsible for ensuring the ICT Services equipment inventory is updated following the moving of any ICT equipment.

6.2.4 Disposal of ICT equipment

6.2.4.1 ICT Services is responsible for the disposal of any piece of ICT equipment which is no longer required by the Council.

7 Legal Responsibilities Policy

7.1 Scope

7.1.1 The Council collects, holds and uses data about people and organisations with whom it works with in order to conduct its business. This may include members of the public, current, past and prospective employees, clients, customers, contractors, partners and suppliers. In addition, the Council may be required to collect and use personal data in order to comply with its statutory obligations.

7.1.2 Any information **must** be handled properly however it is collected, recorded and used, whether on paper, on a computer, or recorded on other media. Personal information is no exception. There are safeguards in the Data Protection Act 1998 to ensure that personal information is processed correctly.

7.1.3 This policy outlines every user's responsibilities under the Data Protection Act 1998 and other relevant legislation.

7.1.4 The Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998, and other relevant information security legislation. Therefore, the Council will ensure that all employees and contractual third parties of the Council who have access to any information held by or on behalf of the Council are fully aware of, and abide by, their duties and responsibilities under this legislation.

7.1.5 This policy aims to mitigate the following risks:

- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of incorrect use of personal information or the failure to comply with legal requirements.
- Potential legal action against the Council or individuals as a result of incorrect use of personal information.
- Reputational damage to the Council as a result of incorrect use of personal information or its failure to meet legal requirements.

7.2 Applying the Legal Responsibilities Policy – Data Protection

7.2.1 Data Protection Act

7.2.1.1 The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

7.2.2 What are the Principles of Data Protection?

7.2.2.1 The Data Protection Act 1998 stipulates that anyone processing personal data **must** comply with **Eight Principles** of good practice. These Principles are legally enforceable.

7.2.2.2 The Principles require that personal information:

- **must** be fairly and lawfully processed;

- **must** be processed for limited purposes;
- **must** be adequate, relevant and not excessive;
- **must** be accurate and up to date;
- **must not** be kept for longer than is necessary;
- **must** be processed in line with the data subject's rights;
- **must** be secure;
- **must not** be transferred to other countries without adequate protection.

7.2.2.3 The Data Protection Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data. Sensitive personal data is defined as:

"personal data consisting of information as to:

a) the racial or ethnic origin of the data subject,
b) his political opinions,
c) his religious beliefs or other beliefs of a similar nature,
d) whether he is a member of a trade union,
e) his physical or mental health or condition,
f) his sexual life,
g) the commission or alleged commission by him of any offence, or
h) 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.

7.2.2.4 The data subject also has rights under the Data Protection Act. These consist of:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances;
- The right to take action for compensation if they suffer damage by any contravention of the Act by the data controller; and
- The right to correct, rectify, block or erase information regarded as wrong information.

7.2.3 How will the Council ensure Compliance with the Data Protection Act?

7.2.3.1 In order to ensure it meets its obligations under the Data Protection Act, the Council will ensure that:

- There is an individual with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are legally responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.
- Queries about handling personal information are promptly and courteously dealt with.

- Methods of handling personal information are regularly assessed and evaluated.
- Appropriate advice is available to Council employees.

7.2.4 Roles and Responsibilities

7.2.4.1 The Council's Data Protection Officer will provide guidance and advice to employees to facilitate the correct handling of personal information and to enable the Council to meet its legal obligations under the Data Protection Act.

7.2.4.2 The Council's Data Protection Officer is responsible for notifying the Information Commissioner's Office of the Council's purposes for processing personal information.

7.2.4.3 Heads of Service are responsible for ensuring that the Council's Data Protection procedures are communicated and implemented within their area of responsibility.

7.2.4.4 Managers are responsible for ensuring that all their staff are appropriately trained with regards to Data Protection and for ensuring that any Data Protection related issues in their own area are handled in compliance with this policy and relevant procedures.

7.2.4.5 Managers are responsible for ensuring that all personal data is disposed of securely and in line with the Retention Guidelines for Local Authorities.

7.2.4.6 All Council employees **must** attend relevant Data Protection training.

7.2.4.7 All Council employees are responsible for understanding, and adhering to this policy and any Council procedures relating to Data Protection.

7.2.4.9 All Council employees should seek Data Protection advice from the Council's Data Protection Officer when necessary.

7.2.5 Sharing Personal Information with other Organisations

7.2.5.1 Personal information classed as PROTECT or RESTRICTED **must not** be disclosed to any other person or organisation via any insecure method.

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

7.2.5.3 The Council's Data Protection Officer is responsible for the Information Sharing Protocol and any Data Exchange Agreements.

7.3 Applying the Legal Responsibilities Policy – Freedom of Information Act

7.3.1 The Freedom of Information Act gives the public a general right of access to information held by public authorities. The Act also requires public authorities to have an approved publication scheme which is a means of providing access to information which an authority proactively publishes.

7.3.2 All Council employees have a duty to provide advice and assistance, so far as is reasonable, to anyone who has made, or proposes to make, a request for information. The Council generally has 20 working days to respond to a request for information.

7.3.3 PROTECT or RESTRICTED non-personal information **must not** be disclosed to any other person or organisation before the information asset owner is consulted and advice sought from the Council's Monitoring Officer to establish whether the information can be disclosed. The information asset owner **must** ensure the information is unclassified and re-marked before the information is disclosed.

7.3.4 Roles and Responsibilities

7.3.4.1 The Council's Freedom of Information Officer will provide guidance and advice to employees to enable the Council to meet its legal obligations under the Freedom of Information Act.

7.3.4.2 The Council's Freedom of Information Officer is responsible for publishing the Council's publication scheme and Managers are responsible for ensuring the information held in the publication scheme is kept up-to-date.

7.3.4.3 Heads of Service are responsible for ensuring that the Council's Freedom of Information procedures are communicated and implemented within their area of responsibility.

7.3.4.4 Managers are responsible for ensuring that all their staff are appropriately trained with regards to Freedom of Information and for ensuring that any Freedom of Information requests are dealt with in accordance with the Freedom of Information Act.

7.3.4.5 All Council employees **must** attend appropriate Freedom of Information training and abide by this policy and the relevant guidance relating to Freedom of Information. Ensuring that the Council responds to requests for information promptly is a shared responsibility.

7.3.4.6 All Council employees should seek Freedom of Information advice from the Council's Freedom of Information Officer when necessary.

7.4 Applying the Legal Responsibilities Policy – Environmental Information Regulations

7.4.1 The Environmental Information Regulations provide members of the public with the right to access environmental information held by public authorities.

7.4.2 Environmental information covers:

- The state of the elements of the environment, such as air, water, soil, land, fauna (including human beings)
- Emissions and discharges, noise, energy, radiation, waste and other such substances
- Measures and activities such as policies, plans ands agreements affecting or likely to affect the state of the elements of the environment
- Reports, cost-benefit and economic analyses
- The state of human health and safety, contamination of the food chain
- Cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment)

7.4.3 The Council generally has 20 working days to respond to a request for environmental information.

7.4.4 Roles and Responsibilities

7.4.4.1 The Council's Environmental Information Regulations Officer will provide guidance and advice to Council employees to enable the Council to meet its legal obligations under the Environmental Information Regulations.

7.4.4.2 Heads of Service are responsible for ensuring that the Council's Environmental Information Regulations procedures are communicated and implemented within their area of responsibility.

7.4.4.3 Managers are responsible for ensuring that all their staff are appropriately trained with regards to Environmental Information Regulations and for ensuring that any requests for environmental information are dealt with in accordance with the Environmental Information Regulations.

7.4.4.4 Managers are also responsible for making environmental information available to the public and to publish facts and analyses of facts which are considered relevant and important in framing major environmental policy proposals.

7.4.4.5 All Council employees **must** abide by the relevant Council guidance and procedures relating to the Environmental Information Regulations.

7.4.4.6 All Council employees should seek Environmental Information Regulations advice from the Council's Environmental Information Regulations Officer when necessary.

8 Information Security Incident Management Policy

8.1 Scope

8.1.1 This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

8.2 Applying the Information Security Incident Management Policy

8.2.1 Reporting information security incidents

8.2.1.1 Information security incidents need to be reported at the earliest possible stage as they need to be quickly assessed by the Head of ICT Services

8.2.1.2 The definition of an “information security incident” is an adverse event that has caused or has the potential to cause damage to the Council’s assets, reputation and / or personnel.

8.2.1.3 An information security incident includes, but is not restricted to, the following:

- The loss or theft 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.

8.2.1.4 Examples of some of the more common forms of information security incidents have been provided in the Appendix.

8.2.1.5 Information security incidents, for example a virus infection, could quickly spread and cause data loss across the Council. All users **must** contact the ICT Service Desk if they notice anything unusual on their computer.

8.2.1.6 All users **must** report any suspected information security incidents immediately to the ICT Service Desk. Users should provide as much information as possible including:

- 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.

8.2.1.7 If the information security incident is in relation to personal information, whether on paper or electronic, the Council's Data Protection Officer will be informed.

8.2.1.8 Information security incidents reported to application and service providers by users **must** also be reported internally to the ICT Service Desk.

8.2.1.9 The Head of ICT Services will be informed of all information security incidents.

8.2.2 Analysing information security incidents

8.2.2.1 A consistent approach to dealing with all information security incidents events will be maintained across the Council.

8.2.2.2 All information security incidents will be analysed by the Head of ICT Services. The level of impact of an information security incident will be determined as per the Council's Risk Management Strategy.

8.2.2.3 If an information security incident requires information to be collected for an investigation the Head of ICT Services will contact Internal Audit for guidance and ensure that any processes are adhered to.

8.2.2.4 The Head of ICT Services will report all high and medium rated risk information security incidents to the Council's Monitoring Officer.

8.2.3 Management of Information Security Incidents and Improvements

8.2.3.1 Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

8.2.3.2 The Head of ICT Services will maintain an incident management process covering identifying, assessing, managing and monitoring information security incidents and including the collection of any evidence that might be required for analysis as forensic evidence.

8.2.3.3 ICT Services will ensure only identified and authorised staff have access to the affected systems during the incident and that all of the remedial actions are documented in as much detail as possible.

8.2.4 Learning from Information Security Incidents

8.2.4.1 The ICT Managers will regularly review information security incidents at a Post Incident Review. The types and volumes of incidents and costs incurred during the incidents will be analysed to identify any patterns or trends.

8.2.4.2 The Head of ICT Services will share this analysis, where appropriate, with the Warning, Advice and Reporting Point (WARP) to aid the alert process for the region.

Appendix - Examples of Information Security Incidents

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.
- Sending a sensitive e-mail to 'all staff' by mistake.
- 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 equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's User id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying PROTECT or RESTRICTED information and not storing it appropriately.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any Council computer equipment.

9 Removable Media Policy

9.1 Scope

9.1.1 This policy should be adhered to at all times, but specifically whenever any user intends to store or transfer any information used by the Council to conduct official business on removable media devices.

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

- CDs.
- DVDs.
- USB storage devices
- 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).

9.1.3 Securing PROTECT or RESTRICTED information (referred to in the Council's Information Protection Policy) is of paramount importance – particularly in relation to the Council's need to protect personal information in line with the requirements of the Data Protection Act 1998.

9.1.4 This policy aims to mitigate the following risks:

- Disclosure of PROTECT and RESTRICTED information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Reputational damage to the Council as a result of information loss or misuse.

9.1.5 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 the Council's 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 PROTECT and RESTRICTED information.
- Prohibit the disclosure of information as may be necessary by law.

9.1.6 ICT Services 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 ICT equipment for the purposes of conducting official Council business.

9.2 Applying the Removable Media Policy

9.2.1 Restricted Access to Removable Media

9.2.1.1 It is Council policy to prohibit any removable media devices being connected to the Council's computer systems or network. The use of such removable media devices will only be approved if there is a valid business case for its use. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks **must** be demonstrated before approval is given.

9.2.1.2 Requests for access to, and use of, removable media devices **must** be made to the ICT Service Desk via the Use of Removable Media Request form. Approval for their use needs to be given by the Council's Data Protection Officer if the request relates to the processing of personal information. All other requests will be handled by an ICT Manager.

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

9.2.2 Procurement of Removable Media

9.2.2.1 All removable media devices and any associated equipment and software **must** only be purchased and installed by ICT Services Non-council owned removable media devices **must not** be used to store any information used to conduct official Council business.

9.2.3 Security of Data

9.2.3.1 Removable media should not be the only place where data required for Council purposes is held. Copies of any data stored on removable media devices **must** also remain on the Council's network as all data on the Council's network is backed up regularly.

9.2.3.2 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 whilst in their care or under their control.

9.2.3.3 Users should be aware that ICT Services will log / audit the transfer of data files to and from all removable media devices and Council-owned ICT equipment.

9.2.4 Incident Management

9.2.4.1 Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the ICT Service Desk.

9.2.5 Third Party On-site Access to Council Information

9.2.5.1 No third party (external contractors, partners, agents, the public or non-employee parties) may use removable media devices to extract information from the Council's computer systems without explicit agreement from the Head of ICT Services.

9.2.5.2 Should third parties be allowed access to Council information then all the considerations of this policy apply to their storing and transferring of the data.

9.2.6 Preventing Information Security Incidents

9.2.6.1 ICT Services will ensure all data on removable media devices is scanned using virus and malware checking software before the removable media is connected to the Council's network.

9.2.6.2 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 Council, other organisations or individuals from the data being lost whilst in transit or storage.

9.2.7 Disposing of Removable Media Devices

9.2.7.1 Removable media devices that are no longer required, or have become damaged, **must** be returned to the ICT Service Desk.

9.2.7.2 All data on any removable media devices that are to be reused for storing data **must** be deleted by ICT Services. Users are responsible for returning the removable media devices to the ICT Service Desk.

9.2.8 Users Responsibilities

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

- All PROTECT and RESTRICTED data stored on removable media devices **must** be protected by encryption.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices **must not** to be used for archiving or storing records as an alternative to the Council's network.
- 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.

10 Remote Working Policy

10.1 Scope

10.1.1 This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of Council ICT equipment and personal ICT equipment when working on official Council business away from Council premises (i.e. working remotely).

10.1.2 This policy also applies to all users' use of Council ICT equipment to access Council information systems or information whilst outside the United Kingdom.

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

- Laptop computers.
- Tablet PCs.
- PDAs.
- Palm pilots.
- Mobile phones including Blackberries.
- Text pagers.
- Wireless technologies.

10.1.4 The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves.

10.1.5 Securing PROTECT or RESTRICTED information when users work remotely or beyond the Council network is a pressing issue – particularly in relation to the Council's need as an organisation to protect information in line with the requirements of the Data Protection Act 1998.

10.1.6 This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to PROTECT and RESTRICTED information.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

10.2 Applying the Remote Working Policy

10.2.1 User's Responsibilities

10.2.1.1 It is the user's responsibility to ensure that the following points are adhered to at all times whilst they are responsible for Council owned portable computer devices.

10.2.1.2 Users **must** take due care and attention of portable computer devices in transit.

10.2.1.3 Users **must not** install or update any software on to the portable computer device.

10.2.1.4 Users **must not** install any screen savers on to the portable computer device.

10.2.1.5 Users **must not** change the configuration of any portable computer device.

10.2.1.6 Users **must not** install any hardware to or inside any portable computer device, unless authorised by ICT Services.

10.2.1.7 Users **must** allow ICT Services access to the portable computer device to undertake any maintenance work.

10.2.1.8 Data should be stored on the Council's network wherever possible and not held on the portable computer device. If data is stored on the portable computer device it must be backed up onto the Council's network as soon as possible.

10.2.1.9 Users **must** immediately report any faults with, damage to, loss or theft of, the portable computer device to the ICT Service Desk.

10.2.1.10 Users **must not** remove or deface any asset registration number.

10.2.1.11 The ICT equipment can be used for personal use by employees so long as it is not used in relation to an external business. Also personal use by employees **must not** be during work time.

10.2.1.12 No family members may use the ICT equipment. The ICT equipment is supplied for the employee's sole use.

10.2.1.13 Users **must** ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, the Council may recover the costs of repair.

10.2.1.14 Users should seek advice from the ICT Service Desk before taking any Council supplied ICT equipment outside the United Kingdom.

10.2.1.15 ICT Services may at any time, and without notice, request a software or hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users **must** co-operate fully with any such audit.

10.2.1.16 Users choosing to undertake work at home or remotely in relation to their official duties using their own IT equipment should understand that they are not permitted to process any PROTECT or RESTRICTED information relating to the Council, its employees, or customers.

10.2.1.17 **Under no circumstances** should PROTECT or RESTRICTED information be emailed to a private non-Council email address.

10.2.1.18 Users accessing GCSx type services or facilities, or using GCSx PROTECT or RESTRICTED information, **must** only use Council-owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely.

10.2.1.19 Users shall ensure that appropriate security measures are taken to stop unauthorised access to PROTECT or RESTRICTED information, either on the portable computer

device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as the Council itself.

10.2.1.20 Users should ensure portable computer devices are switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

10.2.1.21 Users **must** ensure all PROTECT or RESTRICTED data held on portable computer devices is protected by encryption.

10.2.1.22 Users **must** comply with all the appropriate information security policies and relevant guidance notes.

10.2.2 Managers Responsibilities

10.2.2.1 Managers **must** inform the ICT Service Desk of any authorised remote workers and which systems they require access to.

10.2.3 Remote and Mobile Working Arrangements

10.2.3.1 The Council's ICT 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.

10.2.3.2 Users **must** ensure that user identification information is kept in a separate location to the portable computer device at all times. Any removable media devices and paper documentation **must not** be stored with the portable computer device.

10.2.3.3 Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Waste paper containing PROTECT or RESTRICTED information **must** be disposed of in the Council's confidential waste bins.

10.2.4 Access Controls

10.2.4.1 ICT Services will provide appropriate security measures to allow remote users to access Council systems by connecting over public networks such as the Internet.

10.2.4.2 ICT Services will ensure that dual authentication is used when accessing the Council network and information systems (including Outlook Web Access) remotely via both Council owned and non-Council owned equipment.

10.2.5 Anti Virus Protection

10.2.5.1 ICT Services will deploy an up-to-date Anti Virus signature file to all users who work away from the Council premises. Users who work remotely **must** ensure that their Council owned portable computer devices are regularly connected to the Council's network to enable the Anti Virus software to be updated.

11 IT Infrastructure Security Policy

11.1 Scope

11.1.1 This policy applies to all users of the Council's owned or leased / hired computer facilities and equipment. The policy defines what paper and electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved.

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

11.1.3 The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council's information. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access.

11.1.4 This policy aims to mitigate the following risks:

- Unauthorised access to Council information.
- Unauthorised misuse or destruction of Council information.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of unauthorised access to PROTECT and RESTRICTED information.
- Potential legal action against the Council or individuals as a result of unauthorised access to PROTECT or RESTRICTED information.
- Council reputational damage as a result of unauthorised access to PROTECT or RESTRICTED information.

11.2 Applying the IT Infrastructure Security Policy

11.2.1 Secure Areas

11.2.1.1 Information Asset Owners **must** ensure PROTECT and RESTRICTED information is stored securely. A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored.

11.2.1.2 The Councils must ensure that their buildings have appropriate control mechanisms in place for the type of information and equipment that is stored there.

11.2.1.3 Access to secure areas **must** be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should challenge anyone not wearing a badge or equivalent identification tag. Each team **must** ensure that doors and windows are properly secured.

11.2.1.4 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.

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

11.2.1.6 ICT Services will ensure keys to all secure areas housing ICT equipment are held securely and not stored near these secure areas.

11.2.1.7 Where an information security breach occurs, or a Council employee leaves outside normal termination circumstances, the employee's manager is responsible for ensuring that all identification and access tools/passes (e.g. badges, keys etc.) are recovered from the Council employee and arranging for any door/access codes to be changed immediately.

11.2.2 Non-Electronic Information Security

11.2.2.1 Information asset owners are responsible for ensuring all PROTECT or RESTRICTED information is stored securely. For example, using the controls

- Filing cabinets that are locked with the keys stored away from the cabinet.
- Locked safes.
- Stored in a Secure Area protected by access controls.

11.2.3 ICT Equipment Security

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

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

11.2.3.2 Users **must not** store Council information on the local hard drive of their desktop computer. Information should be stored on the Council's network where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained. Users should refer to the Managing your Information guidance Note for guidance concerning network drives and the appropriate place to store Council information.

11.2.3.3 The ICT Technical Team will ensure all servers are 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 the Head of ICT Services

11.2.3.4 The ICT Support Team will record all items of ICT equipment on the ICT Services equipment inventory. The ICT Support Team will ensure the inventory is updated as soon as Council computer assets are received, moved or disposed of.

11.2.3.5 The ICT Support Team will ensure all Council ICT equipment is security marked and has a unique asset number allocated to it. This asset number will be recorded in the ICT Services equipment inventory.

11.2.3.7 The ICT Technical Team will ensure all network cabling is protected against interception or damage.

11.2.4 Equipment Maintenance

11.2.4.1 ICT Services and users **must** ensure that all of the Council's ICT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. The ICT Service Desk will:

- Retain all copies of manufacturer's instructions.
- Identify recommended service intervals and specifications.
- Enable a call-out process in event of failure.
- Ensure only authorised technicians complete any work on the equipment.
- Record details of all remedial work carried out.
- Identify any insurance requirements.
- Record details of faults incurred and actions required.

11.2.4.2 The ICT Service Desk will maintain a service history record of equipment so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

11.2.5 Security of Equipment Off Premises

11.2.5.1 The Council's Removable Media policy requires the use of removable media to be formally approved by the user's manager. ICT Services also has some ICT equipment that can be borrowed for use on site / off site. Any requests to borrow ICT equipment should be made to the ICT Service Desk.

11.2.5.2 Equipment taken away from Council premises is the responsibility of the user and should:

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

11.2.5.3 Users should ensure that they are aware of and follow the requirements of the Council's insurance policy for any Council ICT equipment taken off site. Any losses / damage to this equipment **must** be reported to the ICT Service Desk.

11.2.6 Secure Disposal or Re-use of ICT Equipment

11.2.6.1 Users must return any Council ICT equipment that is no longer required to the ICT Service Desk.

11.2.6.2 ICT Services will ensure any ICT equipment that is to be reused or disposed of has all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) ICT Services **must** ensure the data removal is achieved by using professional data removing software tools.

11.2.6.3 ICT Services will ensure all software media is destroyed appropriately to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

11.2.7 Delivery and Receipt of ICT Equipment into the Council

11.2.7.1 In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following **must** be applied:

- ICT equipment deliveries **must** be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note.
- The ICT Service Desk must be informed immediately of any receipt of ICT equipment and this should be collected without delay and the delivered items should be checked again against the delivery note.
- ICT Services will ensure all new ICT assets are recorded in the ICT equipment inventory.

11.2.8 Regular Audit

11.2.8.1 The Head of ICT Services will arrange for regular independent audits of the Council's information security arrangements and lead on any recommended information security improvements where necessary.

12 User Information Security Standards Policy

12.1 Scope

12.1.1 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 Council employee that initiates this third party access.

12.1.2 The Council understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Council information systems **must**:

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

12.1.3 This policy **must** therefore be applied prior, during and after any user's access to information or information systems used to deliver Council business.

12.1.4 Access to Council information systems will not be permitted until the requirements of this policy have been met.

12.1.5 This policy aims to mitigate the following risks:

- Disclosure of PROTECT and RESTRICTED information as a consequence of loss, theft or careless use of Council information systems.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

12.1.6 The procedures accompanying this policy are split into 3 key stages of a user's access to information or information systems used to deliver Council business:

1. Prior to granting access to information or information systems - checks **must** be made to ensure that the individual is suitable for access to Council information systems.

2. The period during access to information or information systems - users **must** be trained and equipped to use systems securely and their access **must** be regularly reviewed to ensure it remains appropriate.

3. When a user's requirement for access to information or information systems ends (i.e. when a user terminates their employment with the Council, or changes their role so that access is no longer required) - access needs to be removed in a controlled manner.

12.2 Applying the User Information Security Standards Policy – Prior to Employment

12.2.1 Roles and Responsibilities

12.2.1.1 Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of their manager and the appropriate System Administrator.

12.2.1.2 Managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the ICT Service Desk in a timely manner, using the IT Access Form.

12.2.1.3 The information security responsibilities of users **must** be defined and documented and incorporated into induction processes and contracts of employment.

12.2.2 User Screening

12.2.2.1 Background verification checks **must** be carried out on all potential users, in accordance with all relevant laws, regulations and ethics. The level of such checks **must** be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.

12.2.2.2 Managers **must** ensure that potential users are recruited in line with the Council's recruitment policy for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those users.

12.2.2.3 Managers **must** ensure users who require access to the Government Connect Secure Extranet (GCSx) and email facility are cleared to the "Baseline Personnel Security Standard" (BPSS).

12.2.2.4 Managers **must** ensure users who require access to systems processing payment card data, credit checks on the user are carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

12.2.3 Terms and Conditions of Employment

12.2.3.1 As part of their contractual obligation users **must** agree and sign the terms of their employment contract, which shall state their and the Council's responsibilities for information security.

12.2.3.2 Each user **must** sign a confidentiality statement or equivalent that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

12.3 Applying the User Information Security Standards Policy – During Access to Information or Information Systems

12.3.1 During Continued Employment

12.3.1.1 All users **must** sign the Information Security Policy Acceptance form confirming they understand, accept and will abide to the Council's information security policies. This must be done when a new or amended information security policy is released.

12.3.1.2 Managers **must** notify the ICT Service Desk in a timely manner of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate.

12.3.1.3 The ICT Service Desk **must** ensure processes are in place so that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

12.3.1.4 Managers **must** ensure users understand and are aware of information security threats and their responsibilities in applying appropriate information security policies.

12.3.2 Information Security Awareness, Education and Training

12.3.2.1 All users **must** undertake appropriate information security awareness training and keep abreast of regular updates in related statute and organisational policies and procedures as relevant for their role.

12.3.2.2 Managers **must** ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

12.4 Applying the User Information Security Standards Policy - When Access to Information or Information Systems is No Longer Required

12.4.1 Secure Termination of Employment

12.4.1.1 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 the Council's information assets is removed in a timely manner when no longer required by the user.

12.4.2 Termination Responsibilities

12.4.2.1 Managers **must** notify the ICT Service Desk in a timely manner of the impending termination or suspension of employment so that their access can be suspended or removed.

12.4.2.2 The ICT Service Desk **must** notify the appropriate System Administrators who must suspend or remove access for that user at an appropriate time, taking into account the nature of the termination.

12.4.2.3 Managers **must** ensure users return all of the Council's ICT assets in their possession upon termination of their employment, contract or agreement.

12.4.2.4 The ICT Service Desk **must** ensure processes are followed to ensure that all access rights of users of Council information systems are removed in a timely manner upon termination or suspension of their employment, contract or agreement.

12.4.2.5 The ICT Service Desk **must** ensure processes are in place to enable emergency suspension of a user's access when that access is considered a risk to the Council or its systems as defined in the Information Security Incident Management Policy.

13 GCSx Acceptable Use Policy

13.1 Scope

13.1.1 This policy **must** be adhered to at all times when accessing GCSx facilities.

13.1.2 This policy and statement supplements the Council's Email Acceptable Usage Policy.

13.1.3 GCSx mail **must** be used for sending external emails containing PROTECT and RESTRICTED material. All emails sent via GCSx **must** use an "@east-northamptonshire.gcsx.gov.uk" or "@wellingborough.gcsx.gov.uk" email account as appropriate.

13.1.4 This policy aims to mitigate the following risks:

- Disclosure of PROTECT and RESTRICTED information as a consequence of incorrect use of secure email.
- Unauthorised use of secure email.
- Potential legal action against the Council or individuals as a result of the illegal use of secure email.
- Reputational damage to the Council as a result of misuse of secure email.

13.2 Applying the GCSx Acceptable Usage Policy

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

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

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

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

4. 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,

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

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

7. 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,

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

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

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

11. will appropriately mark, using the Council's Protective Marking System Criteria; information sent via the GCSx; and,

12. will not send PROTECT or RESTRICTED information over public networks such as the Internet; and,

13. will always check that the recipients of e-mail messages are correct so that potentially sensitive or PROTECT or RESTRICTED information is not accidentally released into the public domain; and,

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

15. will not forward or disclose any sensitive or PROTECT or RESTRICTED 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,

16. will seek to prevent inadvertent disclosure of sensitive or PROTECT or RESTRICTED information by avoiding being overlooked when working, by taking care when printing information received via GCSx (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,

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

18. will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via GCSx (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,

19. where ICT 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,

20. will make myself familiar with the Council's security policies, procedures and any special instructions that relate to GCSx; and,

21. will inform the ICT Service Desk immediately if I detect, suspect or witness an incident that may be a breach of security as stated in the Information Security Incident Management Policy; and,

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

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

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

25. will not introduce viruses, Trojan horses or other malware into the system or GCSx; and,

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

27. will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant referred to in the Council's Legal Responsibilities Policy; and,

28. 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 Information and Records Management Policy.

14 Communications and Operation Management Policy

14.1 Scope

14.1.1 This policy should be applied whenever users access the Council's ICT facilities and equipment, and especially when managing, developing, configuring or maintaining the Council's ICT facilities and equipment.

14.1.2 This policy covers the key areas in day to day operations management of the Council's ICT services. Its purpose is to clarify the specific arrangements around core ICT processes and procedures, including referencing more detailed documents where applicable.

14.1.3 This policy aims to mitigate the following risks:

- Disruption to normal operations caused by unplanned changes to any part of the Council's data network
- Data loss through insufficient backup arrangements being in place
- Data loss through insufficient data destruction procedures being in place
- Service downtime caused by hardware or software failure
- Malicious attack of the Council's network from viruses, individuals or via un-patched software
- User activity is not fully auditable throughout the network

14.2 Applying the Communications and Operation Management Policy

14.2.1 Operational Procedures and Responsibilities

14.2.1.1 Documented Operating Procedures

14.2.1.1.1 System Administrators will ensure operating procedures are used in all day to day maintenance of the Council's ICT systems and infrastructure in order to ensure the highest possible service from these assets. System Administrators will ensure these operating procedures are documented to an appropriate level of detail for the intended audience.

14.2.1.2 Change Management

14.2.1.2.1 System Administrators will ensure all changes to the Council's operational systems are controlled with a formally documented change control procedure. The change control procedure should include references to:

- A description of the change and business reasons.
- Information concerning the testing phase.
- Impact assessment including security, operations and risk.
- Formal approval process.
- Communication to all relevant people of the changes.
- Procedures for aborting and rolling back if problems occur.
- Process for tracking and audit.

14.2.1.2.2 ICT Services will ensure all significant changes to the main infrastructure (e.g. Network, Directories) are assessed for their impact on information security as part of the standard risk assessment.

14.2.1.3 Separation of Development, Test and Operational Facilities

14.2.1.3.1 The ICT Technical Team will ensure the development and test environments are separate from the live operational environment to reduce the risk of accidental changes or unauthorised access. The environments must be segregated by the most appropriate controls including, but not limited to, the following:

- Running on separate computers, domains, instances and networks.
- Different usernames and passwords.
- Duties of those able to access and test operational systems.

14.2.2 System Planning and Acceptance

14.2.2.1 Capacity Planning

14.2.2.1.1 The ICT Technical Team will ensure all Council ICT infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

14.2.2.1.2 Key ICT infrastructure components include, but are not restricted to, the following:

- File servers.
- Domain servers.
- E-mail servers.
- Web servers.
- Printers.
- Networks.
- Environmental controls including air conditioning.

14.2.2.2 System Acceptance

14.2.2.2.1 Users and ICT Services must ensure any new information systems, product upgrades, patches and fixes undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorisation.

14.2.2.2.2 Users and ICT Services must ensure all major system upgrades are thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

14.2.2.3 Protection against Malicious and Mobile Code

14.2.2.3.1 The ICT Technical Team will ensure all appropriate steps are taken to protect all Council ICT systems, infrastructure and information against malicious code by running effective and up-to-date anti-virus software on all servers and PCs.

14.2.2.4 Patching

14.2.2.4.1 The ICT Technical Team will ensure all servers have appropriate critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. Patches must be applied to all software on the Council network where appropriate.

14.2.2.4.2 The ICT Technical Team will ensure unpatchable software is not used where there is a GCSx connection provided.

14.2.2.4.3 The ICT Technical Team will adhere to the Council's Patch Management Procedure and keep a full record of which patches have been applied and when.

14.2.2.5 Controls against Malicious and Mobile Code

14.2.2.5.1 Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:

- ActiveX.
- Java.
- JavaScript.
- VBScript.
- Macros.
- HTTPS.
- HTML.

14.2.2.5.2 The ICT Technical Team will put in place appropriate access controls (e.g. administration / user rights) to prevent installation of software by all users in order to prevent malicious and mobile code.

14.2.2.5.3 The ICT Technical Team will ensure anti-malware software is installed on appropriate points on the network and on hosts.

14.2.3 Backups

14.2.3.1 Information Backup

14.2.3.1.1 The ICT Technical Team will ensure regular backups of essential business information are taken to ensure that the Council can recover from a disaster, media failure or error. An appropriate backup cycle will be used and fully documented. Any 3rd parties that store Council information must also be required to ensure that the information is backed up.

14.2.3.1.2 The ICT Technical Team will ensure full backup documentation, including a complete record of what has been backed up along with the recovery procedure, is stored at an off site location in addition to the copy at the main site and be readily accessible. This will be accompanied by an appropriate set of media tapes and stored in a secure area. The remote location will be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

14.2.3.1.3 The ICT Technical Team will ensure appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

14.2.3.1.4 The ICT Technical Team will ensure documented procedures are kept for backup tapes that are removed on a regular rotation from Council buildings. Media stores must be kept in a secure environment.

14.2.3.1.5 The ICT Technical Team will ensure backup retention schedules are defined in the Council's IT Disaster Contingency and Recovery Plans.

14.2.3.2 Information Restore

14.2.3.2.1 The ICT Technical Team will ensure full documentation of the recovery procedure is created and stored. Regular restores of information from back up media will be tested to ensure the reliability of the back up media and restore process and this should comply with the agreed change management process.

14.2.4 Physical Storage Media in Transit

14.2.4.1 Users **must** ensure storage media being transported is protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate, physical controls such as encryption or special locked containers should also be used.

14.2.5 Security of System Documentation

14.2.5.1 System Administrators **must** ensure system documentation is protected from unauthorised access. Examples of the documentation to be protected include, but are not restricted to, descriptions of:

- Applications.
- Processes.
- Procedures.
- Data structures.
- Authorisation details.

14.2.5.2 Effective version control should be applied to all documentation and documentation storage.

14.2.6 Monitoring

14.2.6.1 Audit Logging for Restricted Data and GCSx Services

14.2.6.1.1 The ICT Technical Team will ensure audit logs are kept for a minimum of six months which record exceptions and other security related events. As a minimum audit logs must contain the following information:

- System identity.
- User ID.
- Successful/Unsuccessful login.
- Successful/Unsuccessful logoff.
- Unauthorised application access.
- Changes to system configurations.
- Use of privileged accounts (e.g. account management, policy changes, device configuration).

14.2.6.1.2 The ICT Technical Team will ensure access to the logs is protected from unauthorised access that could result in recorded information being altered or deleted. System Administrators will be prevented from erasing or deactivating logs of their own activity.

14.2.6.2 Administrator and Operator Logs

14.2.6.2.1 The ICT Support Team, ICT Technical Team and System Administrators **must** maintain a log of the systems activities. The logs should include:

- Back-up timings and details of exchange of backup tapes.
- System event start and finish times and who was involved.
- System errors (what, date, time) and corrective action taken.

14.2.6.2.2 The logs should be checked regularly to ensure that the correct procedures are being followed.

14.2.7 Clock Synchronisation

14.2.7.1 The ICT Technical Team will ensure all computer clocks are synchronised to the GSI time source to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation.

14.2.8 Network Management

14.2.8.1 Network Controls

14.2.8.1.1 The ICT Technical Team will ensure connections to the Council's network infrastructure are made in a controlled manner. Network management is critical to the provision of Council services and must apply the following controls:

- Operational responsibility for networks should, where possible be separate from computer operations activities.
- There must be clear responsibilities and procedures for the management of remote equipment and users (please refer to the Remote Working Policy and Removable Media Policy.
- Where appropriate, controls must be put in place to protect data passing over the network (e.g. encryption).

14.2.8.1.2 The ICT Technical Team will ensure the network architecture is documented and stored with configuration settings of all the hardware and software components that make up the network. All components of the network should be recorded in an asset register.

14.2.8.1.3 The ICT Technical Team will ensure all hosts must be security hardened to an appropriate level. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

14.2.9.2 Wireless Networks

14.2.9.2.1 The ICT Technical Team will ensure wireless networks apply controls to protect data passing over the network and prevent unauthorised access and that encryption is used on the network to prevent information being intercepted. WPA2 should be applied as a minimum.

14.2.10 Protection of System Test Data

14.2.10.1 System Administrators will ensure that If personal information is used during the development and test phase of preparing application software it is protected and controlled in line with the Data Protection Act and where possible depersonalised. If operational data is used controls must be used including, but not limited to, the following:

- An authorisation process.
- Removal of all operational data from the test system after use.
- Full audit trail of related activities.
- Any personal or confidential information must be protected as if it were live data.

14.2.11 Annual Health Check

14.2.11.1 The ICT Infrastructure Manager will ensure an annual health check of the Council's ICT infrastructure systems and facilities is undertaken every 12 months. This health check must include, but is not restricted to, the following:

- A full penetration test.
- A network summary that will identify all IP addressable devices.
- Network analysis, including exploitable switches and gateways.
- Vulnerability analysis, including patch levels, poor passwords and services used.
- Exploitation analysis.
- A summary report with recommendations for improvement.

5.0 Policy Compliance

5.1 The Councils recognise that there are risks associated with users accessing and handling information in order to conduct official Council business. Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss, reputational damage, and an inability to provide necessary services to its customers**.**

5.2 If any user is found to have breached this policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

5.2 If any Council employee does not understand the implications of this policy or how it may apply to them, they should seek advice from their manager.

5.3 The Council's Strategic Management Team can authorise suspension to access the Council's information systems where misuse is suspected in accordance with the Council's disciplinary procedure.

6.0 Review and Revision

6.1 This policy will be reviewed as it is deemed appropriate or every three years by the Head of ICT Services. This review will include consultation with relevant stakeholder groups and an equalities impact assessment.

Appendix 1 Information Security Policy Acceptance

I have read and understood the information security policies. **I accept these policies and understand that failure to comply with these policies may lead to disciplinary action.**		
	User signature	Date
Email Acceptable Use Policy		
Internet Acceptable Use Policy		
Software Policy		
IT Access Policy		
Information Protection Policy		
Computer, Telephone and Desk Use Policy		
Legal Responsibilities Policy		
Information Security Incident Management Policy		
Removable Media Policy		
Remote Working Policy		
IT Infrastructure Policy		
User Resources Information Security Standards		
GCSx Acceptable Use Policy (GCSx users only)		
Communications and Operation Management Policy		

User Name		**ICT use only**
Job Title		
Service		
Manager's Name		
Manager's Signature		
Date		


East
Northamptonshire
Council


Borough Council of
Wellingborough