A453

St Edmundsbury
BOROUGH COUNCIL

ICT

Security

Policy

Version: 7.1
Date: 28th December 2009
Author: A.P.Hainsworth - Systems Development & ICT Security Manager

Index

Appendices

1. Introduction

1.1. The council has a large investment in the use of Information Communications Technology (ICT) which is used to the benefit of all directorates. In many areas of work, the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level which is appropriate for the council's needs.

1.2. This policy should be reviewed at least annually to ensure that new threats and changes in technology have been accounted for.

2. Policy objectives

2.1. There are three main objectives of this policy:

- To ensure that all of the council's assets, users of ICT, data and equipment are adequately protected on a cost-effective basis against any action that could adversely affect the ICT services required to conduct it's business;
- To ensure that users are aware and fully comply with all relevant legislation: and
- To create and maintain within all directorates, a level of awareness of the need for ICT security to be an integral part of the day to day operation, so that all staff understand the need for ICT security and their own responsibilities.

3. Application

3.1. The security policy is relevant to all ICT services irrespective of the equipment or facility in use and applies to:

- All employees, members and agents;
- Employees and agents of other organisations who directly or indirectly support or use the ICT services;
- All use of ICT throughout the council and at home or in other organisations when engaged on council business.

4. Responsibility for Security

4.1. ICT security is the responsibility of the council as a corporate entity and all members of staff. The Management Team and Members have approved this policy.

4.2. The ICT security policy will apply to all staff who use any form of computer facilities. All members of staff are to be issued with security instructions, which will specify their responsibilities and draw their attention to the possible consequences of not complying with the instructions.

4.3. Senior and line managers in all directorates must be responsible for the implementation and policing of the Security Policy and will receive procedural notes to cover the key areas of responsibility.

4.4. All 3rd party providers of ICT services must ensure the security, integrity and availability of data within the service provided.

5. Legislation

5.1. The council has to abide by all UK and European legislation affecting ICT. All council employees and agents must comply with the following Acts and guidelines and they may be held personally responsible for any breach of guidelines, current legislation as listed below, and any future legislation that may be enacted:

- Data Protection Act, 1998
- Copyright Designs and Patents Act, 1988
- Computer Misuse Act 1990
- Freedom Of Information Act 2000
- Requirements and advice of the Information Commissioner on data handling and storage
- Code of Connection (CoCo) in respect of the Government Secure Extranet GCSx

Information about the above Acts can be found on the government website: www.opsi.gov.uk/acts.htm and guidelines on Information Security can be found on: www.ico.gov.uk or from the council's Data Protection Officer (currently a member of the Legal Team).

6. Standards and Procedures

6.1. Physical access

6.1.1. Precautions should be taken to ensure that access to PCs is restricted at all times to authorised personnel.

6.1.2. Equipment should be sited to reduce the risk of damage, interference and unauthorised access.

6.1.3. All equipment including desktop and laptop PCs must be powered off and stored in a secure manner when left in premises which are likely to be unattended e.g. overnight, and should not be left on view in unattended vehicles. When laptops are left in the office they should be locked away.

6.1.4. All appropriate computer equipment will be identity tagged and be recorded on the central ICT & e-Services' inventories. It is the responsibility of line managers to notify the ICT & e-Services Section of any movements or changes.

6.1.5. Where computer equipment is to be used away from council buildings e.g. when mobile working or for use at home:

- The council's current policy regarding homeworking must be adhered to and it is the responsibility of the individual in whose care the device is to ensure the safety and security of both the equipment and any data contained thereon.
- All of the provisions of this policy document apply.
- When using any equipment outside the UK, caution should be exercised especially if handling sensitive data.

6.1.6. No equipment purchased, leased or hired by a user department may be connected to the council's network or attached to any equipment connected to the network without authorisation from Management Team or its delegated officers. The restriction also applies to any equipment not owned, leased or hired by the council. This includes, but is not limited to: USB memory sticks, ipods®, digital cameras, iPhones, BlackBerry® and other smart phones.

6.2. System Access

6.2.1. Requests to provide access to the network or systems should be made initially through the relevant line manager or section head.

6.2.2. Network passwords will be set to prevent unauthorised access to data held on computer equipment. The use of Boot passwords is especially important in the case of laptop/notebook PCs which are highly portable and less physically secure. Users must not disclose their password to anyone. However, in some exceptional cases a shared PC may have a network password known by several users within an office to enable access. Where this is unavoidable, adequate mechanisms should exist to ensure access to the PC is solely by authorised personnel.

6.2.3. Unique usernames will be allocated by the system administrators. Wherever possible, these will be consistent across applications. Access levels will be determined and implemented by systems administrators for each application area. Likewise access to any shared resource on the network e.g. printers, can be given by the network administrators.

6.2.4. Terminals/PCs should not normally be left 'logged in' when unattended. Where this does occur it should be ensured that either an authorised screensaver with password or time-out facilities are in operation. If staff know they are leaving sight of their desk for any period, they should 'lock' their workstation, which not only blocks any sensitive information from view, but also prevents access with the relevant password to 'unlock' the terminal.

6.2.5. A corporate 'null' screensaver will be provided giving immediate complete screen confidentiality and should be used in conjunction with a password. This will automatically be set after a maximum duration of 10 minutes. Unauthorised screensavers are not permitted as they can cause unacceptable overloading of pc's and the network.

6.2.6. Passwords should be used to protect all systems and should not be written down or disclosed to others not properly authorised to use them.

Employees will be held liable for any misuse of a computer resulting from use of their password/username.

6.2.7. Passwords must be changed to a previously unused password at least every 3 months in line with existing council policy, see appendix A on Passwords. Passwords should be set wherever possible to automatically expire if not changed at this frequency, e.g. log on to the network.

6.2.8. Passwords should normally be specific to individual staff and comprise a minimum of 6 alpha/numeric characters arranged in such a fashion that they will not easily be guessed.

6.2.9. System Administrators must be promptly notified of all leavers to enable the timely removal of all access rights.

6.3. Information & Data

6.3.1. Information held on the council's ICT facilities or subsequent output, e.g. printed letters/tabulations, is the property of the council and is governed by the provisions of the Data Protection Act. Any purpose for which personal information is held about people, must be registered under the Act by the council's Data Protection Officer.

6.3.2. Information and data held or transmitted, e.g. via e-mail, is subject to the National Protective Marking Scheme as explained in Appendix E. Data marked '**Restricted**' or above must **not** be sent outside the council unless encrypted or when using the Government Secure Extranet – GCSx.

6.3.3. Information held should only be released to authorised persons and ICT facilities supplied must only be used for authorised purposes. ICT facilities should normally only be used for official purposes. Occasional and reasonable personal work is permitted. Such activity must not prejudice or interfere in any way with the council's ICT facilities nor its business activities. Any such use should be carried out in staff's own time, and be approved by their line manager. Excessive use or use for commerce or personal gain is not permitted.

6.3.4. Any personal or sensitive data displayed upon unattended equipment must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so. This is applicable to information displayed on visual display units, printed output and computer produced media such as microfiche.

6.3.5. Under no circumstances must any data that contains personal or sensitive information be stored on local devices e.g. c:\ drives, mobile devices such as laptops, PDAs or USB memory sticks. The ICT & e-Services section have guidelines to help staff avoid placing unnecessary and unwanted data in the wrong place. You can find this in Appendix B and on the public network drive area under 'Q:\FAQ\general\User Filestore - FAQ.pdf'

6.3.6. Users with 'Roaming' profiles should be aware that each time they log onto a PC their profile, including copies of their 'desktop' and contents of 'My Documents' are downloaded to the PC and remain there after logging off. These are updated each time they return to use the device so, as well as adhering to 6.3.4., such 'locally' stored data should be kept to a minimum.

6.3.7. No information of a personal or sensitive nature shall be sent outside the council unless authorised. In which case the data must be encrypted. For guidance on how this can be achieved, contact the ICT & e-Services Help Desk.

6.3.8. All data held on the council's network or any device used by staff and agents should only be held for a period appropriate to its relevance and erased or destroyed in line with the council's Data Retention Policy found on the intranet under Freedom of Information.

6.3.9. All computer output no longer required by the council should be disposed of with due regard to its sensitivity. Confidential output should be disposed of by shredding or placed in secure bins located in strategic positions for secure pulping. Microfiche shredded, CD-ROMs scratched, floppy discs and other magnetic media should have data erased.

6.3.10. Any queries relating to the provisions of the Data Protection Act and how it affects your operations should be directed via your line manager to the council's Data Protection Officer.

6.3.11. Users are responsible for setting file or folder permissions to ensure data is only accessible to the relevant authorised staff. Training and advice on this is coordinated by ICT & e-Services.

6.4. **Virus Protection**

6.4.1. All PCs (including laptops/notebooks) should be protected by virus protection software which is upgraded regularly by the ICT & e-Services Section. Any detected viruses must be reported to the ICT Help Desk immediately.

6.4.2. All disks/CD-Roms/USB Memory sticks or other USB devices will be virus checked automatically prior to use in any of the council's computers. This is especially relevant where disks have been received from an external source.

6.4.3. Disks/CD-ROMS/USB Memory sticks or other USB devices must not be inserted into PCs until after the boot or initial password has been entered and the computer has reached:

- The point where you log into the network, or
- The windows screen on stand-alone PCs.

6.4.4. The licence with the council's current supplier of virus protection software permits and recommends free use of the software on any current member of staff's home PC, particularly where there is any

chance of the member of staff using their own PC for work purposes. Copies of the software are available on request from ICT & e-Services Section.

6.5. Software copyright

6.5.1. The copying of proprietary software programs or associated copyrighted documentation is prohibited and is an offence that could lead to personal criminal liability with the risk of a fine or imprisonment.

6.5.2. The loading of proprietary software programs for which a licence is required but not held is prohibited and this is also an offence which could lead to a large fine or imprisonment. All software system disks and licences must be held by the ICT & e-Services Section.

6.5.3. Personal software e.g. games, must not be loaded on the council's computers under any circumstances. If the software is deemed to be of use to the council, then it should be duly acquired under licence.

6.5.4. Spot checks may be conducted by the ICT & e-Services Section and/or Audit Section personnel to ensure compliance with these provisions. Authorised personnel from both sections have rights of access to all systems, the power to seek explanations from members of staff concerned and the right to remove any unauthorised software found to have been installed.

6.6. Computer misuse

6.6.1. All employees should be aware of their access rights for any given hardware, software or data and must not attempt to experiment or attempt to access hardware, software or data for which they have no approval or need to conduct their duties.

6.6.2. Staff are required to comply with any E-mail and Internet usage policy issued on behalf of the council.

6.7. Contingency planning

6.7.1. Security copies (back ups) should be taken at regular intervals dependant upon the importance and quantity of the data concerned. In the case of systems and data residing on network servers, the ICT & e-Services Section will take them on behalf of users at appropriate intervals.

6.7.2. In the case of networked personal computers, the prime copy of all data files must be held on the network file server(s). Advice on changing the default(s) from the local C drive on PCs to space on the appropriate server, normally the Z drive is available from the ICT & e-Services Section, but it is the responsibility of individual members of staff to place their data files in the relevant location.

6.7.3. In the case of applications running locally, users must ensure that all data is backed-up either across the network or where this is not possible, on local back-up media which can be obtained through the ICT & e-Services Help Desk where required.

6.7.4. Arrangements must be in place and procedures specified by the relevant Business Unit Manager in conjunction with the ICT & e-Services Manager, to ensure critical systems/operations are able to continue in the event of complete computing failure.

6.7.5. Security copies should be stored away from the system to which they are related in a restricted access fireproof location. Security copies should be regularly tested to ensure that they enable the system/relevant file to be reloaded in an emergency.

6.7.6. Security copies should be clearly marked as to what they are and when they were taken. Depending on importance of the system concerned, they should provide for system recovery at various different points in time over a period of several weeks.

6.8. Acquisition and disposal of ICT Products

6.8.1. All acquisitions should be in accordance with the provisions of the council's ICT strategy and its financial regulations. Any queries should be directed to your Head of Service or the ICT & e-Services Manager.

6.8.2. The disposal of ICT equipment **must be** co-ordinated through the ICT & e-Services Section who will arrange for the permanent removal of all data and software licensed to the council unless the recipient is taking over the licence and is authorised to use it.

6.8.3. The disposal or permanent handover of equipment, media or output containing personal or sensitive data **must be** arranged in a way that ensures confidentiality.

6.8.4. Disposal should be in accordance with the provisions of financial regulations.

6.8.5. Wherever possible, consideration is given to the re-allocation of equipment within the Council.

6.9. Suspected security incidents, loss or theft of equipment and data.

6.9.1. It is the duty of all members of staff to report any suspected security incidents immediately. Such information shall be regarded as confidential by all employees involved, and should be reported to the Audit Section, ICT Security Manager, Data Protection Officer, Insurance Officer and any other Senior Officer as deemed appropriate.

6.9.2. If any device has been lost or stolen and is one of the council's laptops that uses VPN access, the ICT Security Manager will immediately ensure that the VPN account is disabled.

6.9.3. When such an incident is reported, the ICT Security Manager will conduct an immediate investigation with the appropriate head of service to establish whether any data lost is of a personal or sensitive nature and any consequential business risk it poses to the council. The Audit Team will also conduct an investigation to establish whether there has been a breach of this policy or any other relevant rules or statute and whether appropriate action must be taken.

6.9.4. Where a data breach is identified to have compromised an individual or set of individuals, those individuals must be notified as soon as possible and steps taken to minimise the risk of potential fraud or loss to the individuals affected.

6.9.5. Any data breach shall also be investigated and if necessary the office of the Information Commissioner informed by the council's Data Protection Officer and a full report of the incident with a list of actions taken and a plan of future preventative steps required to be taken to reduce risk of recurrence shall be submitted to CMT by the ICT Security Manager.

6.9.6. A checklist of the actions in section 6.9 can be found in Appendix C.

7. Violations

7.1. Violations of this ICT security policy may include, but are not limited to, any act that:

- Exposes the council, its members, staff or customers to actual or potential monetary loss through the compromise of ICT security;
- Involves the disclosure of confidential information or the unauthorised use of corporate data;
- Involves the use of data for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body.
- Fall within the terms of Computer Misuse in section 6.6 above.

8. Disciplinary process

8.1. The council views computer security seriously and any breach of this policy could lead to disciplinary or legal action being taken against those who commit a breach. Violations such as the use of unauthorised software, the use of data for illicit purposes or the copying of software which breaches copyright agreements will normally be considered gross misconduct.

9. Acknowledgements

Computer Audit Guidelines – Cipfa

IT Policies & Procedures – GEE Publishing Ltd

Various Suffolk Districts within the Suffolk IT Forum.

Appendix A.

POLICY ON USE AND CONTROL OF PASSWORDS

The following rules on the use of passwords apply to all systems in use within the authority.

a) Network Passwords must be a **minimum** of **7 characters**, one of which should be numeric.

b) Network Passwords must contain characters from three of the following four categories:
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Base 10 digits (0 through 9)
   - Non-alphabetic characters (for example, !, $, #, %)

c) Your password cannot contain your username or parts of your full name that exceed two consecutive characters. **Names** that are likely to be easily associated with the user, spouses, children's or pet's names for example, **should be avoided**.

d) You will not be allowed to re-use any of your previous 20 Network Passwords

e) Passwords must **not** be **written down** and left in the vicinity of the user's work area.

f) The system will prompt you to **change** your Network Password every 70 days.

g) Section or Department heads should ensure that passwords known to staff that leave the authority's employ are changed immediately on their departure.

h) Where possible, applications should be set to force a change of password at regular intervals.

Notes

For the majority of applications the ability to change passwords lies directly with the end user; this allows **you** to change **your own** password. Where this is not the case this function is carried out by the system controller, who will ensure that passwords are changed for you.

Some systems are set to force users to change passwords after a set period of time; the time period can be varied with the assistance of ICT & e-Services staff.

Section or Department heads are responsible for ensuring compliance with the policy.

These measures are for the protection of **your** data; it is therefore in your own interest to ensure that this policy is adhered to.

If you have any queries relating to these measures, please contact the ICT Help Desk.

Appendix B.

ADVICE ON STORAGE OF COMPUTER FILES

Where should I NOT store files?

On the local hard disc (Drive C),
"My Documents" (unless you have set it to be redirected to a network drive).
The "Windows Desktop"

Why should I not use the above locations? These locations are not secure and if the PC is lost or stolen data can be misused. These locations are not routinely backed up centrally. Therefore if the hard drive on your PC was to fail, or you delete a file, we will not be able to recover them from the central backups.

If you want to access files from your desktop create a shortcut to the file on the network drive. To create a shortcut, right click on the file, select SEND TO, then left click on "Desktop (Create Shortcut).

If necessary, it is possible to create copies of files or folders. To do this laptop users can set up Off-line synchronisation. You can select folder contents to be available when you are not connected to the network. When you are connected to the main network and logon or off these files will synchronise in both directions. Under no circumstances must this be used for personal or sensitive data. If you are in any doubt about what is classed as sensitive data, get guidance from your line manager or the council's Data Protection Officer (currently a member of the Legal Team).

What are the default network drives?

i.e. where users can conceivably store files but the decision as to which drive is appropriate must be taken according to the nature, sensitivity, and need to enable access to other users – not all drives are appropriate for all types of data.

M Drive - Also known as the Geographical Information area. This is where the common data for Mapinfo and Swiftmap is located.

Q Drive - Also known as the Public area. If you wish to share work amongst staff from several departments you may create a folder here and place work in it. Remember to set the folder permissions to allow access only to those staff to whom you wish access it, by default EVERYONE can access data.

V Drive - also known as the Department drive. (e.g. Finance, Chief Execs, Planning …). This will allow you, dependent upon the folder permissions to access the Section Folders. This is mainly there for staff who work for several sections to easily move about between the section folders.

W Drive - also known as the Section drive. This is where the majority of your work should be stored and as such you should set the Microsoft applications to default to this location. If you're unclear about how to do this contact the ICT & e-Services Help Desk on 7677 or computer.help@stedsbc.gov.uk

Appendix B.

X Drive - also known as the user's private drive. This is where you should keep personal files, (CVs, PDRs, etc.) Only someone logged on as yourself will be able to access this area. You should NOT store any files here that might require access by other members of staff. These MUST be stored within the W drive.

Z Drive – This is historical, some departments are still using them, most files stored here have no logical structure for the easy retrieval of files. An explanation suggesting how to create a folder structure and file naming convention that will make it easy for anyone to find a document within seconds can be found on the q:\faq\genral\user filestore - faq.pdf!!

Some departments / sections will have other mapped drives for software specific to their section or user.

Appendix C.

Checklist of Actions for Suspected Security Breach

Action	Actionee	Completed
Report any suspected security incidents immediately. Such information shall be regarded as confidential by all employees involved, and should be reported to:	Staff Member	
Audit Section		
ICT Security Manager,		
Data Protection Officer		
Insurance Officer		
Your Head of Service/Line Manager		
GovCert - www.govcertuk.gov.uk	ICT Security Manager	
If any device has been lost or stolen and is one of the council's laptops that uses VPN access, immediately ensure that the VPN account is disabled and not replacement issued before next step (below) is completed.	ICT Security Manager	
Conduct an immediate investigation with the appropriate head of service to establish whether any data lost is of a personal or sensitive nature and any consequential business risk it poses to the council	ICT Security Manager	
Conduct an investigation to establish whether there has been a breach of this policy or any other relevant rules or statute and whether appropriate action must be taken.	Audit Team	
Where it has been established that a data breach has compromised an individual or set of individuals, those individuals must be notified as soon as possible and steps taken to minimise the risk of potential fraud or loss to the individuals affected.	If staff, then HR; If members of the public, then relevant Head of Service	
Investigate any data breach and if necessary inform the Office of the Information Commissioner with a full report of the incident and a list of actions taken.	Data Protection Officer	
Submit a proposal of future preventative steps required to be taken to reduce risk of recurrence to CMT.	ICT Security Manager	

Appendix D. **ICT Security Dos & Don'ts**

DO:

- Keep passwords to yourself
- Change passwords regularly
- Keep your files on Network Drives
- Use 'ctrl', 'alt', 'del' to lock your PC when leaving your desk
- Lock your laptop away if you leave it in your office overnight
- Lock your laptop out of sight in your boot (if you leave it in your car at all!)
- Log off then switch off your PC at the end of each day before you leave
- Report suspected data loss or theft immediately to your line manager
- When travelling away from the office make sure your laptop is secure and not left unattended.

DON'T:

- Tell anyone your password
- Write your password down
- Respond to suspicious e-mails (Spam)
- Store files on 'desktop', 'C:' drive or 'My Documents'
- Send personal or sensitive data via e-mail without encryption
- Leave your laptop on your desk overnight
- Leave your laptop on view in unattended vehicles
- Leave laptops, PDAs, mobile phones on view in public places
- Use USB memory keys or other easy to lose devices to store sensitive data

Appendix E. Extract from GCSx Operational Guide:

National Protective Marking Scheme

The National Protective Marking Scheme

The National Protective Marking System provides a framework for users to share and protect information in an appropriate manner. As can be seen from the table, each protective marking is allocated an appropriate Impact Level (IL). Each IL describes a severity of impact to the UK of protectively marked information being released outside of normal government handling channels. The IL value is used by DSO's when performing a risk assessment on protectively marked information in order to determine how much protection these assets should be given.

Protective Marking	e-Gov Impact Level
TOP SECRET	6
SECRET	5
CONFIDENTIAL	4
RESTRICTED	3
PROTECT	2 1
Unclassified	0

On 28 February 2007 the new sub-national caveat, PROTECT, was introduced. The purpose of PROTECT is to provide a difference in terms of the handling official information which needs to be protected from compromise of confidentiality, integrity and availability to a known level of assurance, but for which the measures required to safeguard National Security information at RESTRICTED are considered not to always meet the direct business need of the organisation. It is envisaged that in some organisations the use of RESTRICTED will be reduced as a consequence. At the LA level and for users of GCSx it is envisaged that most protectively marked information will be of 'PROTECT' in nature.

At a working level the baseline security objectives for PROTECT will be the same as for RESTRICTED, which are:

- Handle, use and transmit with care.
- Take basic precautions against accidental compromise or opportunist attack.

The distinction between the two markings is that PROTECT is not a National Security marking, and there is a revised calculation for asset value, or consequence of compromise. Depending on the severity of the circumstances either RESTRICTED or PROTECT may apply where compromise would be likely to:

- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies.
- Prejudice the investigation or facilitate the commission of crime.
- Disadvantage government in commercial or policy negotiations with others.

N.B. Within the UK Government, CONFIDENTIAL is an explicit marking with clearly defined handling requirements. Sometimes, within certain local authorities 'Confidential' is used as a marking to indicate that information has a requirement for protection (in UK Government terms it is protectively marked). Care should be taken to ensure that information protectively marked with the national CONFIDENTIAL marking should be handled accordingly.

Appendix E. Extract from GCSx Operational Guide:

National Protective Marking Scheme

The PROTECT Classification

PROTECT	Compromise of information would be likely to affect individuals in an adverse manner
Guidelines	• Cause substantial distress to individuals. • Breach proper undertakings to maintain the confidence of information provided by third parties. • Breach statutory restrictions on the disclosure of information.
Principles and Clearance Levels	• Information classified as PROTECT should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the organisation to access PROTECT level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	PROTECT information transmitted across public networks within the UK or across any networks overseas should be encrypted using an approved system.
Electronic Storage	Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: a. User challenge and authentication (username/password or digital ID/Certificate) b. Logging use at level of individual c. Firewalls and intrusion-detection systems and procedures; server authentication d. OS-specific/application-specific security measures.
Electronic Disposal	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Information protectively marked with PROTECT can be spoken about over the telephone.
Manual Transmission	• Within a single physical location. As determined by the DSO. • Transfer between establishments within or outside UK: a. May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word PROTECT is not visible. b. The outer envelope should be addressed to an individual by name and title. PROTECT mail for/from overseas posts should be carried by diplomatic airfreight c. The outer envelope must clearly show a return address in case delivery is unsuccessful. d. In some cases due to the nature of the contents, identifying the originating organisation may be inappropriate and a return PO Box alone should be used.
Manual Storage	• In an office environment, PROTECT material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

Appendix E. Extract from GCSx Operational Guide:

National Protective Marking Scheme

Descriptors must be used to ensure the marking is correctly applied:

- APPOINTMENTS e.g. a visit to the LA from the HRH Queen Elizabeth II.
- HONOURS e.g. a member of the staff being given an award.
- LOCSEN e.g. locally sensitive information.
- MANAGEMENT e.g. information for the LA senior management team.
- MEDICAL e.g. medial information on an individual.
- PERSONAL e.g. personal information.
- REGULATORY e.g. white papers etc.
- STAFF e.g. organisational staff only.
- ORGANISATIONAL e.g. organisation staff and contractors.

Example: PROTECT LOCSEN would mean that information would have to be protected under the PROTECT marking and the information it contained would be Locally Sensitive (LOCSEN) e.g. closure of a local hospital.

The RESTRICTED Classification

RESTRICTED	Compromise of information would be likely to affect the national interests in an adverse manner
Guidelines	• Affect diplomatic relations adversely. • Hinder the operational effectiveness or security of the UK or friendly forces. • Affect the internal stability or economic well-being of the UK or friendly countries adversely.
Principles and Clearance Levels	• Information classified as RESTRICTED should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the organisation to access RESTRICTED level or above is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	• All RESTRICTED information transmitted across public networks within the UK or across any networks overseas must be encrypted using an approved system.
Electronic Storage	• Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: a. User challenge and authentication (username/password or digital ID/Certificate) b. Logging use at level of individual c. Firewalls and intrusion-detection systems and procedures; server authentication d. OS-specific/application-specific security measures.
Electronic Disposal	• Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Organisations should already be aware from S(E)N 06-10 issued on 22 September 2006 that telecommunications made at RESTRICTED (Confidentially IL 3) level can no longer be guaranteed as secure. Appropriate secure communications should be used.

Appendix E. Extract from GCSx Operational Guide:

National Protective Marking Scheme

RESTRICTED	Compromise of information would be likely to affect the national interests in an adverse manner
Manual Transmission	• Within a single physical location. As determined by the DSO. • Transfer between establishments within or outside UK: a. May be carried by ordinary postal service or commercial courier firms, provided the envelope/packages is closed and the word RESTRICTED is not visible. b. The outer envelope should be addressed to an individual by name and title. RESTRICTED mail for/from overseas posts should be carried by diplomatic airfreight. c. The outer envelope must clearly show a return address in case delivery is unsuccessful. d. In some cases due to the nature of the contents, identifying the originating organisation may be inappropriate and a return PO Box alone should be used.
Manual Storage	• In an office environment, RESTRICTED material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

Major Differences Between PROTECT and RESTRICTED

For LAs the two protective markings which will be most commonly seen in the workplace are PROTECT and RESTRICTED. Out of these two protective markings it is anticipated that PROTECT will be the most common.

Information with the PROTECT protective marking will be handled in the same way as RESTRICTED in most circumstances.

The primary difference is that LAs will be allowed to have telephone conversations with regard to information protectively marked as PROTECT. Information protectively marked as RESTRICTED is not allowed to be passed over the telephone.

Where to find Help?

For all questions regarding security, users' first point of call should be to review local security documents and policies. Following this, users should defer to the DSO. If the DSO cannot answer they query then MPS should be consulted.