'Happy children aiming high!'

New Hartley First School

'A very caring and nurturing school in which the well-being of every child is paramount.'
'The quality of education continues to be good.'
Ofsted, June 2016

ICT and Information Security

Status: **Non - Statutory**

Created/Reviewed **Autumn 2013, 2015**

Next Review: **Autumn 2017**

Introduction

This document sets out the School policy, which is directly in line with Northumberland Council's policy, towards the use of ICT and Information Security.

The purpose of this Policy is to describe the procedures and processes in place to ensure the secure and safe use of the Council's network and its resources and to protect Council systems and data from unauthorised access or disclosure.

Any queries arising from this Policy or its implementation can be taken up directly with the Information Security Officer at ITSecurity@northumberland.gov.uk

The Information Security Officer is the Owner of this document and has approved management responsibility for its development, review and evaluation.

Summary of Contents:

Scope	**2**
Introduction	**2**
Objectives of the Policy	**3**
Other related policies	**3**
Responsibilities	**3**
Legal compliance	**4**
Violations	**4**
Network Access	**5**
Segregation of duties	**6**
Passwords	**7**
Physical Security	**9**
Portable computer equipment	**10**
Secure areas	**11**
Software installation	**11**

Security Incidents, weaknesses and breaches 12
Virus prevention and control 13
Sending confidential information 15
Termination of employment 16
Disposal of media and equipment 17
Audit and review 18
Key legislation 18

1. Scope

1.1 This policy is intended to be read by all staff for general information and awareness, and makes reference to more detailed information and guidance in additional specific Policies.

1.2 The policy is relevant to all Information and Communications Technology (ICT) services irrespective of the equipment or facility in use and applies to:

1.2.1 All employees and others using the Council's equipment and facilities.

1.2.2 All use of ICT throughout the Council.

1.3 In addition, all Users of ICT and other Council facilities are reminded that there are elements of the General Code of Conduct which also apply.

1.4 The Policy also takes into account the creation, management, processing and sharing of information. Therefore, this is an information security policy which incorporates use of ICT (hardware and software), electronic communication (Email, telephone and fax) and issues relating to the storage and use of data, including confidential information.

1.5 The use of E-mail and the Internet are the subject of separate policies.

2. Introduction

2.1 The Council has a large investment in the use of ICT which is used to the benefit of all groups and service users.

2.2 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 all ICT systems and data are maintained at a level which is appropriate for the Council's needs.

2.3 <u>The policy has three main objectives</u>:

2.3.1 To ensure that all of the Council's assets, staff, equipment and data are adequately protected against any action that could adversely affect the ICT services required to conduct the Council's business, and the accuracy and confidentiality of information held.

2.3.2 To ensure that all staff are aware of and fully comply with all relevant legislation.

2.3.3 To create and maintain within all groups and departments a level of awareness of the need for ICT and information security to be an integral part of day to day operations and the responsibility of all staff to comply with this and other relevant policies.

2.4 This policy has been approved by Members and must be read in conjunction with the Council's Code of Conduct. Unions have also been consulted prior to Members approval.

2.5 Additional related Policies include:

2.5.1 Email Policy, describing the acceptable use of the Council's email system, its operation and its management.

2.5.2 Internet Policy, describing the acceptable use of the Council's Internet service, its operation and its management

2.5.3 Transportation, Transfer and Sharing of Data Policy, describing rules associated with personal and confidential data in transit, and procedures for transferring and sharing data

2.5.4 Mobile Computing Policy, for those using mobile devices such as laptop computers

2.5.5 Homeworking Policy, for those working at or from home.

2.5.6 ICT & Information Security Policies Guidelines for Members

2.5.7 ICT & Information Security Policies Guidelines for Managers, detailing specific responsibilities of group and department senior and line managers.

2.5.8 Data Quality Policy, establishing the need for accurate, reliable information sources.

3. Responsibilities

3.1 All users of ICT systems are required to formally acknowledge receipt of the ICT Security Policy and that they have read and understood its content.

3.2 ICT and information security is the responsibility of the Council as a whole and consequently a responsibility of all members of staff and other authorised users. The policy has been approved and adopted by the Chief Executive.

3.3 Senior and line managers in groups and departments must be responsible for the implementation and policing of the Policy. This is detailed in the

Guidelines for Managers which accompanies this Policy and can be obtained from the Information Security Officer at ITSecurity@northumberland.gov.uk

3.4 All providers and Users of ICT services must ensure the security, integrity, confidentiality and availability of all data they create, process or use. Further information on this can be found in the Data Quality Policy available from the Information Security Officer at ITSecurity@northumberland.gov.uk

3.5 The Council complies with all UK legislation which impacts on ICT. All its employees, agents and other authorised users must comply with the following Acts and may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted:

3.5.1 Copyright Designs and Patents Act, 1988
3.5.2 Computer Misuse Act, 1990
3.5.3 Criminal Justice Act 1988
3.5.4 Data Protection Act, 1998
3.5.5 Electronic Communications Act 2000
3.5.6 European Convention on Human Rights
3.5.7 Freedom of Information Act 2000
3.5.8 Human Rights Act, 1998
3.5.9 Obscene Publications Act 1959
3.5.10 Protection of Children Act 1978
3.5.11 Protection from Harassment Act 1997
3.5.12 Public Interest Disclosure Act 1998
3.5.13 Race Relations Act 1976
3.5.14 Regulation of Investigatory Powers Act 2000
3.5.15 Sex Discrimination Act 1975
3.5.16 Telecommunications Act 1984
3.5.17 Telecommunications (Fraud) Act 1997
3.5.18 Telecommunications (Interception of Communications)(Lawful Business Practice) Regulations 20000

By conforming fully to this policy, Users can be assured that they will be complying with the relevant legislation. See Paragraph 15 below for information on key legislation.

4. Violations

4.1 ICT and information security is viewed seriously by the Council and any breach of this policy could lead to appropriate action being taken against those who commit such a breach. Violations will be addressed under appropriate procedures and may include the Disciplinary Procedure.

4.2 Violations of this Policy will include, but are not limited to, any act which:

4.2.1 Exposes the Council to actual or potential monetary loss through the compromise of ICT security;

4.2.2 Involves the creation, processing or use of any data found to be inaccurate or invalid;

4.2.3 Involves the accessing, creation, processing or use of any data by unauthorised users;

4.2.4 Involves the disclosure of confidential and/ or personal information, the unauthorised use of corporate data and/or the sending of defamatory information;

4.2.5 Involves the creation, use, downloading or transmitting of any data or other material for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body.

4.2.6 Involves unauthorised modification, installation or use of software, or the modification, installation or use of unauthorised software

4.3 Any individual who has knowledge of a violation of this *ICT & Information Security Policy* must report that violation immediately to the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk See the Reporting Security Incidents Procedure for more information.

5. Network Access

5.1 Access to the network, and any equipment, application, database or other resource must be by individual login – i.e. unique user name and password. Other than in very exceptional circumstances, generic login credentials are not permissible.

5.2. All external use of the network must be by named individuals only, authorised by an appropriate manager. Access will only be permitted on completion of the Code of Connection by the manager and the authorised user (in addition to a Confidentiality Agreement where appropriate), and will be by unique user name and password.

5.3 The creation of new accounts is carried out by Information Services on receipt of an online new user form detailing the appropriate access levels and permissions by the Line Manager. Whenever possible the new user form must be submitted not less than 2 weeks prior to the new employee starting work.

5.4 Each individual who is authorised to access the Council network is given a profile which limits his or her access to approved data, files and software.

5.5 If, for the purpose of a special project, an individual requires access beyond their normal profile permissions, special access can be arranged, but only for the duration of the project. Any request for a temporary or permanent variation from the profile must be made to the Information Services Service Desk on (01670 53)3333 and authorised

by an appropriate senior manager using the appropriate online change user form.

5.6. All users must only access, or attempt to access, what is permitted by their profile. If there is any difficulty in accessing files or programmes, the Information Services Service Desk on (01670 53)3333 must be informed as soon as possible.

5.7 If access to a file held in an individual's H:Drive is necessary and that person is not available, e.g. they are off work sick, then the line manager must contact the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk for assistance. The reason for the access, the full name of the file and the identity of the person holding it will be needed.

5.8 As a principle all users must retain their files on their H:Drive. However, each H:Drive is restricted to a capacity of 1GB. Should additional storage space be required the use of shared server space or alternative, appropriate storage media should be considered. Advice on this can be sought from the Information Services Service Desk on (01670 53)3333

5.9 Data stored on a computer's hard drive is not automatically backed up, and may be accessible to anyone switching on the PC. A computer hard drive is therefore not secure and must be seen as a last resort and a temporary, short term solution. Similarly, data must not be stored on non-Council equipment.

5.10 Where a computer is shared by a number of users, it is essential for all users to log off the computer before leaving it. A user is responsible for all work carried out on a computer using their login details, including internet access and email use, whether or not that user was actually using the computer themselves.

5.11 The network will require a password change every 90 days. Any accounts with no activity during a 90 day period will be disabled. A further 90 day period of inactivity will result in the account being deleted. An appropriate manager will be informed, and an offline backup copy of any data will be created.

5.12 Segregation of Duties

5.12.1. Access to systems and applications is restricted according to the role and business requirements of each user. Access rights are established and managed on a need-to-know basis, and agreed by a user's line manager and the owner of the system or application.

5.12.2 Access to systems and applications is at all times by unique user ID. Group ID's are generally not allowed, except by

specific agreement of the Information Security Officer and where relevant Internal Audit.

5.12.3 Within a system or application, segregation of duties must be implemented to prevent accidental or deliberate misuse. Duties or responsibilities which may give rise to a conflict of interest if carried out by the same individual must be separated.

5.12.4. In general, access rights comprise the functions of read, write, delete and execute and these are allocated to each user in respect of each system and application.

5.12.5. Access rights are established through the New User / Change User online process, and where appropriate the Change Control process.

5.12.6. Established access rights must be reviewed twice yearly as a minimum to ensure that access to systems and applications remains appropriate and consistent. A review should also take place after any changes to the system, such as an upgrade.

5.12.7. On receipt of a “Delete User” instruction, access rights to all systems and applications associated with that user must be revoked immediately. Monthly Leaver Reports from the HR department should also be checked against access permissions as a second check.

5.12.8. System Administrator access allows full unrestricted rights to defined systems and applications for management purposes, including the creation and removal of system users. This level of access must be kept to the minimum number of individuals required to enable day-to-day operation and emergency access in the event of a system failure. System Administrator access should be via unique individual ID.

5.12.9. The use of privileges in systems and applications must be allocated in a restricted and controlled manner. Privileges enable users to override some controls within a system, usually for system management purposes, and privileges must be removed when no longer required.

5.12.10 Access to systems and applications by third parties, such as partner organisations or software maintenance/ support personnel, must be subject to completion of the Code of Connection and where appropriate the Confidentiality Agreement. Access by third parties must be restricted to only those systems, or parts of those systems, that are required and must be revoked as soon as it is no longer required.. Access of this kind must comply with the requirements of the Transportation, Transfer and Sharing of Data Policy.

6. Passwords

6.1 Passwords must be used in order to access computers, applications, systems and all other networked resources

6.2 Passwords must be alpha-numeric, and contain at least seven characters of which at least one must be a digit.

6.3 Passwords must not be proper names, birth dates or words that can be found in a dictionary. Network login / user names must not be used in any form (reversed, capitalised, or doubled as a password) nor any other information easily obtained about the User (such as pet names, car registration numbers, telephone numbers etc).

6.4 The same password must not be used for more than one application, system, device or service.

6.5 Network passwords cannot be re-used within 20 password changes

6.6 The network will prompt for a password change every 90 days. However, for additional security, Users should consider changing their password more frequently (preferably every 30 – 40 days) both for network access and for specific systems.

6.7 In summary:

Strong Password Do's and don't's

DO	DON'T
Use a password with mixed-case letters	Use a network login ID in any form
Use a password that contains alphanumeric characters, and include at least one digit and punctuation	Use your first, middle or last name or anyone else's in any form. Don't use your initials, nickname, or anyone else's
Use at least seven characters	Use a word contained in an English or foreign dictionary
Use a seemingly random selection of letters and numbers	Use information easily obtainable about you – phone numbers, car registration plate, pet names etc
Use a password that can be typed quickly without having to look at the keyboard	Use a password of all numbers, dates or a combination
Change passwords regularly – at least every thirty days	Use a sample or a default password

6.8 If a software package comes installed with a default password, that password must be changed immediately after installation.

6.9 Passwords must not be posted in a location accessible by others (such as a note stuck to the monitor, under the keyboard or even in a desk drawer).

6.10 Passwords must NEVER be divulged to or shared with anyone else. There are NO exceptions to this, and If a password is disclosed, and therefore compromised the Information Security Officer must be informed on (01670 53)3309 or at ITSecurity@northumberland.gov.uk . If a user is asked for their password over the telephone by someone purporting to be from Information Services or any outside authority, company or organisation, it must not be given. The name and telephone number of the person requesting the password must be taken and the Information Services Service Desk on (01670 53)3333 must be informed immediately.

6.11 A machine must not be left unattended while logged onto a system unless the password protected screen saver has been activated or the computer has been locked. Automatic password-protected screensavers will be remotely applied across the network, following a period of inactivity of 20 minutes.

6.12 Where files or data need to be shared between individuals the data must be held in a networked, restricted shared folder or other secure environment. The Information Services Service Desk on (01670 53)3333 can advise on this.

6.13 Users must remember that they are at all times responsible for anything undertaken with their user id and password.

6.14 A log file of invalid login attempts will be maintained. Under normal circumstances only three attempts at a password will be allowed before automatically barring access, requiring re-activation via the Information Services Service Desk on (01670 53)3333

6.15 Password changes **by Information Services Support Staff**

This paragraph refers to Information Services support staff only

When a need arises to change a User's password during an on-site support visit, and that User is not available to verbally receive the new password, the following steps must be followed:

6.15.1 Email the Service Desk with PASSWORD CHANGE NOTIFICATION as the subject. The email must provide the User Name (and school name if relevant) and the new password

6.15.2 The User's account must then be changed within Active Directory (or User Manager if relevant in the case of a NT4 Domain user) so that the User must enter a new password when they next log on.

6.15.3 Clear notification must be left on the User's PC that the User must contact the Information Services Service Desk in order to obtain their password. NB – new passwords must not be left with other Users and they must not be written down or left on site in any format.

6.15.4 On curriculum networks in schools, details of account and/or password changes must be emailed to the IT Coordinator. Printed versions of user account details must not be produced. Copies of spreadsheets/databases containing user account details must be accessible only to the IT Coordinator

7. Physical Security

7.1 All hardware devices must bear an asset tag sticker, which must not be removed throughout the life of the device.

7.2 All desktop devices, e.g. PC, printer and scanner, must have adequate precautions taken to protect them against theft and accidental damage in addition to environmental threats and hazards. All manufacturer and supplier instructions and advice must be followed.

7.3 Security precautions should, in the first instance, concentrate on adequate building security and siting of the device in the office, and then may extend to simple lock down devices attached to a desk.

7.4 All ICT hardware purchasing must be coordinated through Information Services. This ensures that equipment in use across the Council is consistent, meets appropriate standards and is compatible with existing equipment and network resources.

Therefore, all purchases of hardware must be made through the Information Services Service Desk on (01670 53)3333 or at cshelpdesk@northumberland.gov.uk The request will then be forwarded to the appropriate team for verification and ordering. Advice on hardware requirements is also available from Information Services, again via the Service Desk.

Information Services cannot guarantee installation, support or servicing of equipment purchased independently.

7.5 All desktop computer equipment should be turned off when not being used for an extended period of time.

7.6 Equipment will be protected centrally by an Uninterruptible Power Supply (UPS) and where necessary controls must be in place to ensure a clean power supply by eliminating the impact of power spikes.

7.7 Portable devices /Removable Media

7.7.1 When not in use all portable devices such as laptop computers must be retained in a secure environment. This may include a lockable store cupboard with controlled access, or lockable metal cabinets in larger alarmed offices, but again with controlled access.

7.7.2 All portable devices must be security marked (etched, UV pen, etc.) as soon as received into a department or service, and then added to the appropriate inventory.

7.7.3 When portable devices are taken off premises all Users must ensure that they take adequate precautions to protect the equipment against theft or accidental damage at all times, e.g. not left visible but locked away.

7.7.4 No portable devices must be left in an unattended vehicle at any time.

7.7.5 Departments and Services must make users aware of insurance arrangements and the user's obligations before allowing the device to be taken off the premises.

7.7.6 Users who travel with Council laptops must make regular backups of data contained on the laptop. Advice on making backups can be obtained through the Information Services Service Desk on (01670 53)3333

7.7.7 Laptop computers must not be connected to the network unless anti-virus software has been updated.

7.7.8 Records must be maintained within each department or service which detail their portable devices including type, serial number and software available, and include provision for signing out and return.

7.7.9 Portable devices must only be used in connection with authorised business use on behalf of the Council.

7.7.10 Portable devices must never contain any more data than is the absolute minimum required.

7.7.11 Further information on the use of portable media can be found in the Transportation, Transfer and Sharing of Data Policy and the Mobile Computing Policy.

7.8 All computer consumables must be retained in a secure environment wherever possible and issued only for Council business. Consumables must not be used for private purposes.

7.9 Secure Areas

7.9.1 Server rooms, data centres and all other secure or sensitive areas must be subject to additional security measures including controlled and authenticated access.

7.9.2 It is recommended that all such areas should also be made secure. All buildings should be alarmed and/or security grilles should be in place where appropriate

7.9.3 See the Physical Entry Controls and Secure Areas Policy for more information.

8. Installation of Software

8.1 Software purchases must be coordinated through Information Services via the Information Services Service Desk on (01670 53)3333 or at cshelpdesk@northumberland.gov.uk

8.2 Only software for which the Council is licensed may be installed upon any Council computer. It is the responsibility of each user to ensure that the correct licensing arrangements are followed when installing software. However, this is assumed to be correct when installation is arranged through Information Services, who will retain records relating to current licences and software packages in use.

8.3 If there is any doubt about software license or authenticity the Information Services Service Desk on (01670 53)3333 or at cshelpdesk@northumberland.gov.uk must be contacted before proceeding with installation.

8.4 Appropriate action will be taken against any user found to have installed software that is not properly licensed or if the software is being used contrary to its license agreement.

8.5 Modifications to existing software are generally discouraged, and in any case must be progressed through Information Services and where appropriate be subject to Change Control procedures.

8.6 In certain circumstances officers of the Council evaluate various items of software on their PC to determine if they would be of benefit to the Council. All officers must follow any conditions laid down by the software provider especially when the evaluation is completed. The Information Services Service Desk on (01670 53)3333 must be contacted if there are any problems in following the set conditions.

8.7 Staff negotiating contracts, under which software is to be written for the Council, must seek to ensure that suitable arrangements are made for copyright to be vested in the Council wherever possible.

9. Security Incidents

9.1 More detailed information about Security Incidents can be found in the Information Security Incident Reporting Procedure

9.2 Security Incidents

9.2.1 A Security Incident is a situation where the security of a PC, a system, an application or the network has been compromised, and may be from an internal or external source.

9.2.2 Examples would include Users who have accessed data or material which their User Profile should have prevented them from seeing, or perhaps accessed a system or application at a user level to which they are not entitled. It could also be the introduction of a virus to a PC and / or the network, or network access by an unauthorised user.

9.2.3 Any individual who becomes aware of a security incident must report it as soon as possible to his or her supervisor for reporting on to the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk

9.3 Security Weaknesses

9.3.1 A weakness is a situation whereby potential for a security incident is identified. A PC may be left unattended, logged into a system without a password-protected screensaver or other locking procedure potentially allowing access by unauthorised users.

Further examples could be the inclusion of too many individuals in a system's Administrator profile or a lack of procedures for signing out laptops or other portable devices to individuals, potentially allowing unidentified and/ or unauthorised use of the equipment.

9.3.2 A weakness does not have to be specifically ICT-related. It could be windows left open close to portable equipment, or a PC monitor displaying potentially sensitive data positioned to face a window.

9.3.3 Any individual who becomes aware of a security weakness must report it as soon as possible to his or her supervisor for reporting on to the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk

9.4 Security Breaches and Violations

9.4.1 A security *breach* is an activity which causes or has the potential to cause the loss, damage or corruption of data. This may be the result of a specific Security Incident, a Security Weakness, a Violation of security policies or procedures or a combination of all three.

9.4.2 A security *violation* is any activity which contravenes the ICT & Information Security Policy and other related policies, procedures and guidelines and may result in a security breach.

9.4.3 Any individual who has knowledge of a violation of this or other associated policies must report that violation as soon as possible to the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk The Information Security Incident Reporting Procedure will be implemented.

9.5 Any security breach or violation of this and other related policies could lead to appropriate action being taken against those who commit such a breach or violation. Violations and breaches will be addressed under appropriate procedures which may include the Disciplinary Procedure.

10 Virus Prevention and Control

10.1 A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus can also transmit itself across a network, spreading the infection to other computers and devices.

10.2 The general term is “malware”, which covers various types of virus, worms, Trojans, and spyware. A virus can cause performance problems or more long term damage to a computer or network.

10.3 Malware is most commonly introduced to a computer through internet downloads and as attachments to emails.

10.4 If a virus is found, or suspected, to be on a machine or external storage media, The Information Services Service Desk on (01670 53)3333 must be informed immediately. Advice will be given as to how to deal with it, and The External Security Incident Control Procedure will be implemented

10.5 From time to time Information Services may notify Users, through email, concerning a particular virus and its effect. All Users must take appropriate action when so notified. Deliberate contravention of such a notification is a potential disciplinary matter.

10.6 Virus Prevention

10.6.1 No equipment capable of processing information, whether desktop or portable, must be implemented on the network without appropriate anti-virus software being installed.

10.6.2 All software must be checked for viruses before installation on any Council device, including computers, laptops and other portable devices.

10.6.3 Where a CDRom, USB memory stick or other storage media are used to transfer files, program or data, from one machine to another it must be virus checked before use, particularly if it is from an external source, a different department or service or from a stand alone machine which may not be fully protected against viruses.

10.6.4 If there is any doubt as to the origin of the files being transferred, they must always be checked for viruses before use.

10.6.5 Networked desktop PCs are updated automatically but other equipment such as laptop computers and other mobile devices need to be updated individually. The Information Services Service Desk on (01670 53)3333 can provide further information.

10.7 Downloading from the Internet

10.7.1 As a matter of principle, files downloaded from the Internet must initially be saved onto the User's hard drive (C: drive) and virus checked before opening or executing. Only when it has been found to be clear of viruses can it then be transferred safely to other areas, such as shared folders and H:Drive folders.

10.7.2 More information on the use of the Internet is available in the Internet Usage Policy.

10.8 Extracting Email attachments

10.8.1 Anti-virus software is installed on the Council network and networked machines. However, as a matter of principle in case of malfunction, attachments to external Emails should be saved onto the hard drive (C: drive) and manually virus checked before being opened.

10.8.2 If there are any doubts about the authenticity or content of an Email or its attachment the Information Services Service Desk on (01670 53)3333 should be contacted immediately for advice prior to opening the file.

10.8.3 More information on the use of the Email System is available in the Email Use Policy.

11. Sending Confidential Information

11.1 More detailed information regarding confidential and personal information can be found in the Data Protection Policy and the Transportation, Transfer and Sharing of Data Policy

11.2 It is the responsibility of all employees of the Council to safeguard the security of confidential and/ or personal data for which they are responsible, or which they access in order to carry out their job. There is also a responsibility to bring to a manager's attention any areas of concern regarding the transfer or transportation of such information.

11.3 As a general rule personal and sensitive corporate data must not be disclosed, transferred, or copied to third parties without authorisation from an appropriate senior officer, who understands the purpose of the request and is aware of the procedures to follow.

11.4 Before making information available to anyone else, employees must make sure that they have the authority to disclose it.

11.5 <u>Providing information by telephone</u>

11.5.1 Information must never be given out over the phone or by any other verbal means unless it is absolutely clear who it is being given to and that they are entitled to the information and are ready and able to accept it.

11.5.2 Care must be taken to ensure that conversations involving confidential and/ or personal information cannot be overheard.

11.5.3 Voicemail messages containing personal information should only be left after due consideration has been given to the security and confidentiality risks involved.

11.5.4 Recorded phone messages containing confidential information must be secured by password access. There should be a deputy and / or group password for times of absence.

11.6 <u>Providing Information by Fax</u>

11.6.1 If sending personal information by fax, pre-programmed speed-dialling must not be used, and top sheets must be clearly marked "Private and Confidential", together with the number of pages being sent and the contact details of the sender.

11.6.2 A time must be agreed with the recipient for the sending of the fax, and confirmation of delivery or non-delivery must be given.

11.6.3 A confirmation sheet should be printed and filed as appropriate. The fax machine should also be checked to ensure that its memory does not retain a record of the transmission.

11.7 Providing Information by Email

11.7.1 Email is not a secure means of communication outside the security of the Council's network and must not be used for sending personal or sensitive corporate data. The Information Services Service Desk on (01670 53)3333 or at cshelpdesk@northumberland.gov.uk can advise on alternative means of transmitting personal and / or confidential information

11.7.2 Even when emailing within the security of the Council network it is important to ensure the name and email address of the recipient is correct, and that a suitable subject line is used which does not include personal information.

11.7.3 The sender must also ensure that the recipient is expecting the information and confirm that it has been received successfully.

11.8 Information transported by surface mail must be protected from unauthorised access and environmental damage. External organisations should be requested to use secure post when forwarding confidential information, using tamper-evident packaging when possible.

11.9 When using internal mail, confidential information must be placed in clearly identifiable envelopes and must be protected from loss and accidental viewing, using lockable storage equipment where appropriate.

11.10 Electronic data physically transported between sites, departments or organisations must be properly packaged and clearly labelled to ensure it is handled correctly, and not corrupted by magnetic fields or other environmental damage.

12. Termination of Employment

12.1 When a user who has network access leaves the employment of the Council the appropriate manager must arrange for the transfer of any necessary files and e-mail folders.

12.2 Where termination is due to ongoing disciplinary action the user's access will be denied with immediate effect.

12.3 The appropriate Line Manager mst notify Information Services, using the relevant online form, that the user is leaving so that the user's login credentials can be removed from the network. This removal will not take place earlier than 28 days after the user has left to allow for the deletion or transfer of files, data and emails within the department. However the user's access rights will be disabled immediately.

12.4 On termination it is the user's responsibility to return all equipment, entry passes, software, documentation (both paper and electronic) and any other Council asset in their possession.

13. Disposal of Media and Equipment

13.1 All PCs which have become obsolete or are surplus to requirement must have their hard disks checked for content. Software that is being transferred to another machine must be uninstalled and all data files must be deleted.

13.2 If equipment is to be sold on to another user or organisation, the following statement must be included and enforced as part of the sale agreement documentation:
This equipment is "sold as seen", and Northumberland County Council does not warrant or offer any assurance as to its functionality and operation.
Northumberland County Council will not provide any support or maintenance in connection with the equipment, nor take responsibility for any defects, and will not be liable for any claims, liabilities, damages, losses, costs or expenses arising out of or in connection with the use of the equipment.

13.3 All data storage devices must be purged of sensitive data before disposal or securely destroyed. Advice on confidential, personal and sensitive data is available from the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk

13.4 All removable media must be rendered unusable before disposal. It should be noted that reformatting does not delete all data from disks and such data can subsequently be recovered using freeware.

13.5 Magnetic tapes containing confidential and/ or personal information must be disposed of by a company or agency which meets Waste Electrical and Electronic Equipment (WEEE) Regulation standards. Other magnetic tapes can be disposed of through the general waste disposal procedure.

13.6 Computer hard disks should be sent for disposal with a company or agency which meets WEEE regulation standards.

13.7 Floppy disks containing confidential and/or personal information must be either reformatted by the user before disposal or sent for disposal in the same way as for hard disks above. Other floppy disks can be reformatted and disposed of either by recycling or through the general waste disposal procedure.

13.8 CD and DVD disks containing confidential and/ or personal information must be re-formatted prior to disposal or re-use. Read-only CDs & DVDs must be rendered unreadable by shredding, scratching, heating or otherwise destroying the disk's surface. Other CD or DVD disks can be disposed of through the general waste disposal procedure.

13.9 All paper records can be disposed of through the Council's general waste disposal procedure. However, paper documents containing confidential and/ or personal information must first be shredded

13.10 Tapes from tape-based telephone answering or dictation machines must be erased before disposal, and consideration given to the shredding, or cutting of the tape.

13.11 Digital telephone answering machines must have message stores cleared by removing the back-up batteries and unplugging the machine from the power supply. Once this is done the machine can be passed on to another user or disposed of through the general waste disposal procedure.

14. Audit and Review

14.1 ICT and information security is managed through the Information Security Officer and is subject to regular audit and review

14.2 This and other related policies is reviewed at least annually to ensure continued relevance, accuracy and compliance with the principles of ISO 27001

14.3 The review process is undertaken jointly by Information Services and Internal Audit, and the process is managed by the Information Security Officer

14.4 The review process incorporates compliance testing of individual practices and procedures

15. Key Legislation

15.1 Data Protection Act 1998

15.1.1 Further information about Data Protection is available in the Council's Data Protection Policy, and also the Transportation, Transfer and Sharing of Data Policy

15.1.2 Data Protection refers to the principles and provisions of the Data Protection Act 1998, which seeks to govern the secure management of personal data, and in particular:

15.1.3 The obtaining of personal data

15.1.4 The storage and security of personal data

15.1.5 The use of personal data

15.1.6 The disposal and/or destruction of personal data

15.2 In Data Protection terms, personal data is information which would enable the identification of any living individual.

15.3 The Data Protection Act is based upon 8 principles, aimed at ensuring that all personal data is:

15.3.1 Fairly and lawfully processed

15.3.2 Processed for limited purposes

15.3.3 Adequate, relevant and not excessive

15.3.4 Accurate and up to date

15.3.5 Not kept for longer than is necessary

15.3.6 Processed in line with the rights of the subject of the data

15.3.7 Secure

15.3.8 Not transferred to other countries without adequate protection

15.4 <u>The Computer Misuse Act 1990</u>

15.4.1 This Act defines specific offences relating to computer "hacking". Even the intent to make knowingly unauthorised access to programmes or data in a computer is an offence if the computer is made to perform some action (which can be as minor as scrolling the display).

15.4.2 Employees who themselves have authorised access do not have the authority to confer or authorise access on others.

15.4.3 It is an offence to incite anyone to confer unauthorised access.

15.4.4 It is an offence to cause unauthorised modification to programmes and data, which includes deliberately introducing a virus.

15.5 The Copyright, Design and Patents Act 1988

15.5.1 This Act specifies offences relating to the illegal copying of computer software.

15.5.2 All organisations have a legal responsibility to ensure all computer software is licensed by the vendor who holds the copyright to the product. Organisations are responsible for maintaining adequate records to prove compliance.

15.5.3 It has to be the policy of any organisation to ensure no copyright material is copied without the owner's consent.

This Act is enforced by organisations such as FAST (Federation Against Software Theft) and BSA (British Software Alliance) who have wide ranging powers to ensure compliance.