St John Fisher Catholic College

with Humanities Specialist Status

humanities

TRINITY
Sixth Form
Succeeding Together

Policy: Information Security Policy

Date: June 2013

Adopted: July 2013

Version control

Version	Author	Date of amendment
1.0	James Wakefield	01/06/13

Information Security Notes:

St John Fisher Catholic College takes very seriously its obligations in the area of Data Security. The Governors and Employees are committed to the continuing development of secure systems and procedures pertaining to the protection of all personal and personal sensitive data held by St John Fisher Catholic College.

All data processing on the part of St John Fisher is notified to the Information Commissioner's Office. All data handling is conducted in accordance with The Data Protection Act 1998. Data availability is subject to The Freedom of Information Act 2000.

Information Security Policy and Procedure is subject to an annual review cycle. Should any amendments be made to the above legislation prior to the updating of this policy as part of the annual review cycle, the legislation will always take precedent.

Due to the complex and changing nature of technology and legislation, St John Fisher Catholic College elected employees will always consult Staffordshire County Council under the terms of the Service Level Agreement where there is any uncertainty relating to any part of the policy or process.

Information Security Policy for St John Fisher Catholic College

Objective

The objective of this Information Security Policy is to protect the information assets processed by St John Fisher Catholic College from all appropriate threats. Compliance with this Information Security Policy is necessary to ensure the confidentiality, availability and integrity of the school's data, and minimise information security incidents.

In support of this Information Security Policy the Head Teacher and Governors accept their role in being fully accountable for information security and are committed to:

- Treating information security as a high priority
- Creating a security aware education environment
- Implementing controls that are proportionate to risk
- Promoting individual accountability for compliance with information security policies and supporting procedures and guidance

This document is written for all staff of St John Fisher Catholic College, although some of the information contained will be relevant to students.

Scope

Information takes many forms.
The scope of this Information Security Policy includes, but is not limited to:

- All information processed by St John Fisher Catholic College electronically or in paper form, including but not limited to:
  - Pupil data and external partner information and reports
  - Operational plans, accounting records and minutes
  - Employee records
- All information processing facilities used in support of St John Fisher's operational activities to store, process and transmit information
- All external parties that provide services to St John Fisher in respect of information processing facilities.

Policy Coverage

This Information Security Policy provides that St John Fisher Catholic College shall ensure that:

- Information shall be protected against unauthorised access
- Information shall be protected against unauthorised disclosure
- Integrity of information shall be maintained
- Information shall be available to authorised users when required
- Statutory and legal obligations shall be met
- Unauthorised use of information assets and information processing facilities shall be prohibited
- Students shall continually be made aware of information security, it's importance to them and how it can impact on their time in school

- Any third parties utilising the St John Fisher Catholic College site or facilities are aware of their responsibilities under this policy
- All breaches of information security, actual or suspected, shall be reported and investigated.
- Controls shall be commensurate with the risks faced by St John Fisher Catholic College.
- This information security policy shall be communicated to all employees for whom information security training shall be regularly given

In support of this Information Security Policy, more detailed security guidance and processes shall be developed for employees, information assets and information processing facilities.

The guidance documents associated with this policy will cover Information Security in schools in the following areas:

- Internet and Email Usage
- Technical Security

Responsibilities

The Head teacher and Governors of St John Fisher Catholic College shall be accountable for ensuring that appropriate security and legal controls are identified, implemented and maintained. They shall be supported in this task by all employees. Students need to be made aware of their responsibilities under this policy, and supported to uphold it.

The Head Teacher and Governors shall appoint a staff member (Mr J Wakefield) who shall be responsible for managing information security at an operational level,

It is the responsibility of all school employees, students and 3rd parties to adhere to school policies.

Non-compliance of the Information Security Policy by any employee shall result in disciplinary action. Non-compliance by 3rd parties shall result in their connection being terminated.

The Head Teacher and Governors must approve this Information Security Policy.

Policy Implementation

The Head teacher and Governors along with the operational manager with responsibility for Information Security at St John Fisher Catholic College must implement such Information Security controls as they see fit for their establishment.

Policy review and maintenance

This Information Security Policy shall be reviewed annually by the Head Teacher and Governors or at other times as dictated by operational needs.

St John Fisher Pupil Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Group / Class

Signed   Date

St John Fisher Parent/Carer Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. **. If you do not sign and return this agreement, you child will not be granted access to school ICT systems.**

Permission Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

Rules for ICT Users - Staff

	Notes
1	You must not use, or try to use, St John Fisher Catholic College's e-mail and internet facilities to create, distribute or display in any form any material that is or may be considered to be illegal, offensive or unacceptable under our rules and policies. It is impossible to give a complete list of what is considered offensive or unacceptable, but the following are included (and in some cases may also be illegal). Anything that: • is pornographic or obscene, or includes any form of sexually explicit humour; • is intimidating, discriminatory (for example, racist, sexist or homophobic) • is defamatory, encourages violence or strong feelings; • is hateful; • is fraudulent; • shows or encourages violence or criminal acts; • may give St John Fisher Catholic College a bad name; or is a deliberate harmful attack on systems St John Fisher Catholic College use, own or manage.
2	Attempts to access unacceptable internet content will be treated the same whether the attempt was successful or not. Terms entered into search engines such as "google" can be recorded and they will be considered as seriously as the content that would result from the search even if the content is blocked.
3	You must not use the e-mail or internet facilities for time-wasting activities, such as chain letters, or for sending private e-mails to everyone on the global address list.
4	To reduce the likelihood of St John Fisher Catholic College being targeted by spam, phishing or potential malicious activities do not use your St John Fisher Catholic College e-mail address for personal activities. This includes when buying personal goods online.
5	You must not use or try to use St John Fisher Catholic College ICT systems to access, without permission, any e-mail that is intended for another member of staff or an e-mail account of another member of staff.
6	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.

7	You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 The Telecommunications Act 1984 Breaches of this legislation may result in disciplinary, civil and/or criminal action.
8	You must follow any local rules determined by the Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the System Manager.
9	You must ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. This includes if you are accessing systems from outside the school including at home. Do not leave you computer logged on, i.e. where data can be directly accessed without password control, when not in attendance.
10	You must not leave any computer unattended if you are accessing school systems on it unless the screen is locked i.e. it requires a password to gain access. This includes if you are accessing systems from outside the school including at home.
11	You must not exceed any access rights to systems or limitations on the use of data imposed on you by the System Manager. The ability to access information or systems is not the same as having authorisation to do so.
12	The System Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a “made up” word, but not obvious or guessable, e.g. surname; date of birth.
13	You must not share your user name and password with **ANYONE** unless specifically authorised to do so by the System Manager, e.g. in cases of shared access.
14	Do not write your password down. You will be directly accountable for any network activity including internet and email use by your account.
15	The System Manager will advise you on what “back ups” you need to make of the data and programs you use and the regularity and security of those backups.

16	To protect against retrospective information security risks you are required to review any removable storage media used by you in your professional duties which may inadvertently contain sensitive information relating to St John Fisher Catholic College, this includes media owned by you. Any media containing any sensitive information should be presented to the Senior ICT Technician who will facilitate the secure removal of the information. The senior ICT Technician will where appropriate assist with the uploading of required materials to the school network. Any suspected or actual computer virus infection must be reported immediately to the System Manager.
17	You must be vigilant for any suspicious ICT activity. You must immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Headteacher.
18	You must be aware that the data you create with St John Fisher Catholic College equipment and systems remains the property of St John Fisher Catholic College. All data must be handled in accordance with any Protective Marking Scheme that may be in place.
19	You must keep all business-related data on the St John Fisher Catholic College network and not on the hard drive of your PC. Data that is stored on the St John Fisher Catholic College network will be backed up on a regular basis
20	You must lock sensitive data (hard copy and disks) away when not in use. When no longer required you must dispose of any sensitive data (disks) via the agreed school channel. This involves presenting disks (including USB or hard drive) containing sensitive data to the Senior ICT Technician who will arrange for a collection by an agreed contractor for safe disposal. Any printed sensitive data (hard copy) must be disposed of using the secure waste disposal bins located in the staff preparation room.
21	You must not store personal data (non St John Fisher Catholic College work) files including but not limited to personal MP3 files, personal photographs, personal music files and personal documents on the St John Fisher Catholic College network or storage media including the personal home drives. St John Fisher Catholic College will not be held responsible for the deletion of any personal data.
22	You must make yourself aware of the contents of all other ICT related policies such as the school's e-safety and social networking policies.
23	You must not copy files that are accessible centrally on the St John Fisher Catholic College network onto your personal home drive on the network unless for amendment after which they must be deleted from the home drive. Wherever possible, work must be kept on shared network drives and not on your home drives

24	You must avoid taking any sensitive data off site be it on a laptop or USB storage device. St John Fisher Catholic College provides secure channels for accessing required data from outside of the network in the form of the SIMS At Home service. St John Fisher Catholic College is committed to developing the scope and range of secure access channels in accordance with the Information Security Policy for the benefit of Students, Parents and Staff. Should you require sensitive data to be taken off site in order to fulfil your professional duties you must discuss this with your line manager who may refer you to a member of the Senior Management Team to discuss the procurement of encrypted storage devices.

Staffordshire County Council - ICT Security Policy for Schools

Rules and Agreements for Staff

Staff Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users – Staff.

Your details

Name:

Job title:

Signature: Date:

Security Guidelines

1. Password Policy

Passwords should be:

- unique
- alphanumeric
- at least 8 characters in length
- regularly changed, recommend at least every 90 days

Passwords should NOT be:

- written down
- easy to guess
- shared with any other people including family and friends.

2. Monitoring Computer Use by Pupils

- Ensure pupil use of computers is visible, make sure there is a responsible person present and monitoring of use in place.
- Consider logging access to the network using software tools, for example RM Tutor.
- Review the layout of the room to ensure there is good 'visibility' of computer activities.
- Publish the ‘Rules of ICT Use’ in all rooms where students are able to access the network, also display them on the screen when the computer is turned on.
- Maintain an audit trail of user activity.

3. Monitoring Computer Use by Staff (especially in sensitive areas)

- Use screensavers with passwords
- Think carefully about the siting / location of equipment
- When disposing of paper output always use the confidential waste bins provided in any circumstance where paper waste is considered confidential. Waste should be considered confidential when it contains information which allows any living individual to be identified.
- Any hardware containing confidential information including floppy disks, computers etc that may contain sensitive or personal information must be disposed of via the Senior ICT Technician who will arrange for secure disposal.
- All staff MUST be aware that their use will be monitored and there should be no expectation of privacy. In signing the Staff Acceptable ICT Use agreement staff acknowledge the above
- No member of staff will have permission to access the network without having signed the Staff Acceptable ICT Use agreement mentioned above.

4. System Backup

- The system must be backed up regularly and checks must be made that the backup has worked. This back up system should be automated.
- Ensure the instructions for re-installing data or files from a backup are fully documented and readily available.
- Store the backup media in a secure media safe
- Periodically test a backup restore to make sure that the process works.

5. Anti Virus Protection

- Ensure that an approved and recommended product is used.
- Make sure there is a process to ensure it is regularly updated and ALL equipment is included, this is especially important for stand-alone PC's, laptops.
- There is a clear procedure for dealing with any actual or suspected infections
- The process of 'cleaning' infections must be documented - this may involve requesting assistance from the Staffordshire Learning Technologies (SLT)

6. Illegal or Inappropriate Use of the Network

- Ensure that there are appropriate procedures in place for auditing access to the network and systems
- Regularly check the network for 'unauthorised' files
- If possible ensure auditing is performed both at the Management System level and also at the Operating System level (see section 11 below)
- Consider using a firewall or proxy server to restrict external activity and access

7. Internet and Email Use

- An Internet and Email Use policy has been adopted for each 'category' of User (Staff and Pupil) and all Users have signed up to it.
- Define and document any local agreements / policies on restricting web sites, access to newsgroups and chat-rooms etc.
- Obtain parental permission ensuring that parents have signed and agreed to the Parent Acceptable Use Agreement.
- Ensure there is a clear process for reporting any access to inappropriate material.
- Restrict specific functions such as the downloading of .exe files.
- Pupil Internet use is supervised
- Implementing limits on inbox sizes, size and types of attachments etc
- Be clear about what is considered 'appropriate' use of email and language
- Use of websites such as ‘dropbox’ and ‘yousendit’ for file storage and transfer are avoided. Staff advised to share files via the network storage area.

8. Documentation

Ensure adequate documentation is available for

- The network infrastructure
- The network systems, hardware, software etc
- Administration procedures
- Housekeeping procedures
- Problem resolution

Ensure support disks, recovery disks, backups etc are available and stored securely.

9. Training

- Training for all staff is undertaken regularly and covers “existing policy refresh” and/or additions to policy and/or procedure.
- Ensure there is adequate training for System Managers and Users
- Introduce 'good practice' guidelines where appropriate e.g. using screen savers with passwords

10. Authentication / Operating System Level Security

- Consider using system policies to provide additional security
- Ensure there is a rigorous policy for approval / removal of Users
- Avoid the use of 'generic' accounts, where their use is unavoidable ensure they are set up only for the duration of the particular requirement.
- Limit the number of Administrator and Manager accounts
- Avoid the use of Groups with Administrator or Manager rights
- Only log on as Administrator or Manager when performing functions requiring this level of access, use an ordinary level User account where this is not required
- Set clear security levels on the network and ensure these are documented and followed
- Restrict access to applications and data areas where appropriate
- Consider using 'read only' access where possible

11. Network Review

- Monitor system downtime, ensure there are support arrangements in place to react to problems with critical equipment or infrastructure
- Monitor performance of the network - ensure there is a process in place to develop and upgrade the network infrastructure and equipment as necessary
- Monitor service disruption - ensure support arrangements are in place to resolve problems in a timely fashion
- Regularly review appropriate documents e.g. Computer Security policy.
- Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent

12. Monitoring Systems Usage

- Monitor the IT systems usage of all system users including internet and email use to make sure that the School's policy is being adhered to. However in order to comply with legislation including the European Convention of Human Rights and Fundamental Freedoms, The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 all users are made aware that their usage will be monitored and why this monitoring is taking place.
- All users are made aware that that the systems they are using are the property of the school and that there can be no expectation of privacy.
- All users are made aware that the school own the e-mail system which means that the school also own all copies of messages created, received or stored on the systems. The users are made aware that no emails will be private, even if marked as "private" and/or "confidential" or with any similar wording.

13. Protective Marking

St John Fisher Catholic College is aware of protective marking and the important role it can play in information security. The Head teacher and Governors are committed to developing a protective marking policy as part of their ongoing commitment to information security.

A protective marking scheme is a way of assigning information to a security level which, in turn, relates to a range of pre-defined controls designed to ensure the information is handled properly.

14. Hardware and Software Inventory

- In order to comply with the School's Financial Regulations, St John Fisher will maintain an inventory of all ICT equipment (however financed) which must be audited at least annually. St John Fisher Catholic College uses software to support this process. The integrity of the ICT equipment Inventory is under development and is being aided by the use of the above mentioned software.

- The use of all private hardware for school purposes must be approved by the System Manager.

- A comprehensive inventory of all software and licence details is maintained and regularly updated as software is acquired or disposed of. If software is used illegally because it is not licensed it could result in a fine or in extreme cases a jail sentence

15. Transferring Data

- Staff must avoid the transfer of sensitive data outside of the school unless this has been expressly agreed by Senior Staff or is being shared with trusted partners who are legal required to protect information we supply to them. Trusted partners include Social Services, Partner Schools and third party software/facilities suppliers including School Comms (parental text and email).

- As part of the development of information security procedures St John Fisher Catholic College require that no personal or sensitive data be stored on USB storage devices, laptops or other removable media such as CDs. This is critical to reducing the security risks. St John Fisher Catholic College requires that data be shared using the network storage facility. St John Fisher Catholic College is currently developing opportunities for staff to access information remotely and in a secure fashion in order that staff are able to continue their normal duties away from the school site where necessary.

- Sensitive data must not be communicated via email.

Backup Strategy for St John Fisher Catholic College

- All data should be backed up at least 3 times each week – for example, Monday, Wednesday & Friday. This will ensure that at least three copies of the data will always be available.

- At least one of the backups should be kept in a separate secure building on the school premises to the schools servers (in case of fire or theft).

- All backups should be checked to ensure that they have been successful.

- A 'Long Term Backup' should be taken at the beginning of each term. This should be kept and not overwritten until the beginning of the next term. This will help protect against data corruption that may go unnoticed for several weeks, during which 'older' backups will have been overwritten by 'newer' ones.

- Differing media are employed in schools for backing up purposes. E.g. Magnetic tapes, hard disks, USB drives. If you suspect your principal backup medium is not working correctly (tape drives can be unreliable), use an alternative, until a member of the Council's SLT Unit has visited to correct the problem.

- Periodically do a restore from a backup to ensure that the process works and all the data has been successfully backed up.

Repair and Disposal of ICT Equipment and Disposal of Waste

Repair
If a piece of ICT equipment is in need of repair, consideration must be given to the sensitivity of any data that may be on the device. If the data on the device is particularly sensitive, then it will need to be removed and placed securely in network storage before the device is handed over for repair.

A written agreement should be in place between the school and any repairer, stating agreed levels of confidentiality and reinforcing the sensitivity of St John Fisher Catholic College’s data.

St John Fisher Catholic College should ensure that any third parties utilised for repairing equipment are registered under the Data Protection Act as personnel authorised to see data, as such they would be bound by the same rules as school staff in relation to not divulging data or making any unauthorised use of it.

Disposal of ICT Equipment
Prior to the transfer or disposal of any ICT equipment the System Manager or an must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

Disposal of Waste
Disposal of waste ICT media such as print-outs, CDs, Hard Drives and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper and CDs will be shredded if any confidential information could be derived from them.