Holbrook Academy

Acceptable Use of ICT Policy

June 2013

Date Approved	Quality and Monitoring Committee	1.7.2013
	Governing Body	10.7.2013
Signed		Jane Gould (Chair of Governors)
Minuted		
Date of Next Review	Quality and Monitoring Committee	Summer Term 2014
	Governing Body	Summer Term 2014

Contents

1. Introduction

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- VLEs and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

At Holbrook Academy we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

2.0 Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the Academy at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Academy business related information; to confirm or investigate compliance with Academy policies, standards and procedures; to ensure the effective operation of Academy ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using Academy ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

3.0 Breaches

A breach or suspected breach of policy by an Academy employee, contractor or pupil may result in the temporary or permanent withdrawal of Academy ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the Academy Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

4.0 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Network Manager and/or the appropriate member of the Senior Leadership Team. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the same.

5.0 Acceptable Use Agreement: Students – Secondary

Secondary Student Acceptable Use - Agreement / eSafety Rules

- I will only use ICT systems in Academy, including the internet, e-mail, digital video, mobile technologies, etc. for Academy purposes.
- I will not download or install software on Academy technologies.
- I will only log on to the Academy network/VLE with my own user name and password.
- I will follow the Academy's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my Academy e-mail address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of an Academy project approved by my teacher.
- Images of students and/or staff will only be taken, stored and used for Academy purposes in line with Academy policy and not be distributed outside the Academy network without the permission of the subjects of the material and my class teacher.
- I will ensure that my online activity, both in Academy and outside Academy, will not cause the Academy, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be

monitored and logged and can be made available to my teachers.

- I understand that these rules are designed to keep me safe and that if they are not followed, Academy sanctions will be applied and my parent/carer may be contacted.

Letter to be signed by Parent/Carer

Dear Parent/ Carer

ICT including the internet, VLEs, e-mail and mobile technologies, have become an important part of learning in our Academy. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Philip Hart, the Academy eSafety Coordinator.

Please complete and return the bottom section of this form to Academy for filing on your child's student file.

This Acceptable Use Agreement contains a summary eSafety Policy.

✂---

Student and Parent/Carer signature

We have discussed this document and …………………………………….........(student name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Holbrook Academy.

Parent/ Carer Signature …….…………………….…………………………… .....

Student Signature………………………………………………………………….

Form …………………………………. Date …………………………………..

6.0 Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in the Academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the appropriate member of the Senior Leadership Team.

- I will only use the Academy's email / Internet / Intranet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Academy or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to students.
- I will only use the approved, secure e-mail system(s) for any Academy business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely. Personal data can only be taken out of the Academy or accessed remotely when authorised by the Principal or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes inline with Academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Academy without the permission of the parent/carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in Academy and outside Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full via our policies section on the Academy or on request.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the Academy

Signature: …… Date ……

Full Name: ……(printed)

Position: ……..

7.0 Computer Viruses

7.1 All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB, CD) must be checked for any viruses using Academy provided anti-virus software before using them.

7.2 Never interfere with any anti-virus software installed on Academy ICT equipment that you use.

7.3 If your machine is not routinely connected to the Academy network, you must make provision for regular virus updates through the IT department.

7.4 If you suspect there may be a virus on any Academy ICT equipment, stop using the equipment and contact the ICT Technician immediately. The ICT technician will advise you what actions to take and be responsible for advising others that need to know.

8.0 Data Security

The accessing and appropriate use of Academy data is something that the Academy takes very seriously.

8.1 Security

- The Academy gives relevant staff access to its Management Information System, with a unique ID and password;
- It is the responsibility of everyone to keep passwords secure;
- Staff are aware of their responsibility when accessing Academy data;
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use;
- Staff have read the relevant guidance documents available on the Academy website;
- Staff keep all Academy related data secure. This includes all personal, sensitive, confidential or classified data;
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight;
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times;
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared printers are used.

9.0 Disposal of Redundant ICT Equipment Policy

9.1 All redundant ICT equipment will be disposed off through an authorised agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

9.2 All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

9.3 Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-gency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

9.4 The Academy will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

9.5 The Academy's disposal record will include:

- Date item disposed of;
- Authorisation for disposal, including:
  - verification of software licensing
  - any personal data likely to be held on the storage media? *
- How it was disposed of e.g. waste, gift, sale;
- Name of person & / or organisation who received the disposed item.

** If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.*

9.6 Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

10.0 E-Mail

Please see separate E-Mail Policy.

11.0 Equal Opportunities

11.1 Students with Additional Needs

The Academy endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the Academy's eSafety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

12.0 eSafety

12.1 Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the Academy. The Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this Academy is Phil Hart who has been designated this role as a member of the senior leadership team. All members of the Academy community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Principal / eSafety Co-ordinator and all governors have an understanding of the issues and strategies at our Academy in relation to local and national guidelines and advice.

This policy, supported by the Academy's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole Academy community. It is linked to the following mandatory Academy policies: child protection, health and safety, home–Academy agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHEE.

12.2 eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The Academy provides opportunities within a range of curriculum areas to teach about eSafety;
- Educating students on the dangers of technologies that maybe encountered outside Academy is done informally when opportunities arise and as part of the eSafety curriculum studied by all students at the beginning of Year 7;
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them;
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities;
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button;
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

12.3 Managing the Academy eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used;
- The eSafety policy will be introduced to the students at the start of each Academy year;
- eSafety posters will be prominently displayed.

13.0 Incident Reporting, eSafety Incident Log and Infringements

13.1 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the appropriate member of the Senior Leadership Team and/or eSafety Co-ordinator.

13.2 eSafety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

Holbrook Academy
e-Safety Incident Log

Details of ALL e-Safety incidents to be recorded by the e-Safety Coordinator. This incident log will be monitored termly by the Principal, Member of SLT or Chair of Governors.

Date & Time	Name of pupil or staff member	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons

13.3 Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Principal. Incidents should be logged.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator;
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

14.0 Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

14.1 Managing the Internet

- The Academy maintains students who will have supervised access to Internet resources (where reasonable) through the Academy's fixed and mobile internet technology;

- Staff will preview any recommended sites before use;
- Raw image searches are discouraged when working with students;
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research;
- All users must observe software copyright at all times. It is illegal to copy or distribute Academy software or illegal software from other sources;
- All users must observe copyright of materials from electronic resources.

14.2 Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience;
- Don't reveal names of colleagues, students or any other confidential information acquired through your job on any social networking site or blog;
- On-line gambling or gaming is not allowed.

It is at the Principal's discretion on what internet activities are permissible for staff and students and how this is disseminated.

14.3 Infrastructure

- Our Academy employs web filtering which is the responsibility of the IT Technician;
- Holbrook Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998;
- Staff and students are aware that Academy based email and internet activity can be monitored and explored further if required;
- The Academy does not allow students access to internet logs;
- The Academy uses management control tools for controlling and monitoring workstations;
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate;
- It is the responsibility of the Academy, by delegation to the IT Technician, to ensure that Anti-virus protection is installed and kept up-to-date on all

Academy machines;

- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the Academy's responsibility, nor IT Technician, to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to either the IT Technician or class teacher for a safety check first;

- Students and staff are not permitted to download programs or files on Academy based technologies without seeking prior permission from the IT Technician;

- If there are any issues related to viruses or anti-virus software, the IT Technician should be informed.

15.0 Managing Other Web 2 Technologies

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the Academy endeavors to deny access to social networking sites to students within Academy;

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are;

- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online;

- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, Academy details, IM/email address, specific hobbies/ interests);

- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals;

- Students are encouraged to be wary about publishing specific and detailed private thoughts online;

- Our students are asked to report any incidents of bullying to the Academy;

- Staff may only create blogs, wikis or other web spaces in order to communicate with students using the VLE or other systems approved by the

Principal.

16.0 Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of Academy and also to be aware of their responsibilities. We aim to regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to Academy;
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on Academy website);
- Parents/carers are expected to sign a Home Academy agreement containing the following statement or similar;
  - → **We will support the Academy approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the Academy community**
- The Academy disseminates information to parents relating to eSafety where appropriate in the form of:
  - Information and celebration evenings;
  - Posters;
  - Website/ VLE postings;
  - Newsletter items;
  - VLE training.

17.0 Passwords and Password Security

17.1 Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures;
- Staff should change temporary passwords at first logon;
- Change passwords whenever there is any indication of possible system or password compromise;
- Do not record passwords or encryption keys on paper or in an unprotected file;
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

17.2 Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Academy's e-safety Policy and Data Security;
- Users are provided with an individual network, email, VLE form and Management Information System log-in username;
- Students are not allowed to deliberately access on-line materials or files on the Academy network, of their peers, teachers or others. Similarly, students are not allowed to use any machine whilst logged in as a member of staff;
- Staff are aware of their individual responsibilities to protect the security and confidentiality of Academy networks, MIS systems and/or VLE, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the Academy network is 16:30;
- Due consideration should be given when logging into the VLE to the browser/cache options (shared or private computer);
- In our Academy, all ICT password policies are the responsibility of the IT Technician. Staff and students are expected to comply with the policies at all times.

18.0 Personal or Sensitive Information

18.1 Protecting Persona, Sensitive, Confidential and Classified Information

- Ensure that any Academy information accessed from your own PC or removable media equipment is kept secure;
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access;
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others;
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person;
- Ensure the security of any personal, sensitive, confidential and classified

information contained in documents you fax, copy, scan or print. This is particularly important when shared printers are used and when access is from a non-Academy environment;

- Only download personal data from systems if expressly authorised to do so by your manager;

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience;

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information;

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

18.2 Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption;

- Store all removable media securely;

- Securely dispose of removable media that may hold personal data;

- Encrypt all files containing personal, sensitive, confidential or classified data;

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

19.0 Safe Use of Images

19.1 Taking Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the Academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the Academy permits the appropriate taking of images by staff and students with Academy equipment;

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the staff device.

19.2 Consent of Adults who work at the Academy

Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file.

19.3 Publishing Student's Images and Work

On a child's entry to the Academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the Academy web site;
- on the Academy's VLE;
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in the Academy's communal areas;
- in display material that may be used in external areas, i.e. exhibition promoting the Academy;
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Currently, only the Principal's PA has authority to upload to the site. Requests for changes to web content should be sent with clear instructions.

19.4 Storage of Images

- Images/films of children are stored on the Academy's network;
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Principal;
- Rights of access to this material are restricted to the teaching staff and

students within the confines of the Academy network/VLE;
- All staff have the responsibility of deleting the images when they are no longer required, or the student has left the Academy.

19.5 Webcams and CCTV

- The Academy uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the Academy. Please refer to the hyperlink below for further guidance;

- We do not use publicly accessible webcams in Academy;

- Webcams in Academy are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults;

- Misuse of the webcam by any member of the Academy community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

    - Consent is sought from parents/carers and staff on joining the Academy, in the same way as for all images

20.0 Academy ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

20.1 Academy ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the Academy's ICT equipment provided to you;

- It is recommended that academies log ICT equipment issued to staff and record serial numbers as part of the Academy's inventory;

- Do not allow your visitors to plug their ICT hardware into the Academy network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available;

- Ensure that all ICT equipment that you use is kept physically secure;

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990;

- It is imperative that you save your data on a frequent basis to the Academy's network drive. You are responsible for the backup and restoration of any of your data that is not held on the Academy's network drive;

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted;

- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles;

- Privately owned ICT equipment should not be used on a Academy network;

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled;

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person;

- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

20.2 Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on Academy systems and hardware will be monitored in accordance with the general policy;

- Staff must ensure that all Academy data is stored on Academy's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted;

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey;

- Synchronise all locally stored data, including diary entries, with the central Academy network server on a frequent basis;

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades;

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support;

- In areas where there are likely to be members of the general public, portable

or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight;

- Portable equipment must be transported in its protective case if supplied.

20.3 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of Academy too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in Academy is allowed. Our Academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The Academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Academy allow a member of staff to contact a pupil or parent/ carer using their personal device;

- Students are allowed to bring personal mobile devices/phones to Academy but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent;

- This technology may be used, however for educational purposes, as mutually agreed with the Principal. The device user, in this instance, must always ask the prior permission of the bill payer;

- The Academy is not responsible for the loss, damage or theft of any personal mobile device;

- The sending of inappropriate text messages between any member of the Academy community is not allowed;

- Permission must be sought before any image or sound recordings are made on these devices of any member of the Academy community;

- Users bringing personal devices into Academy must ensure there is no inappropriate or illegal content on the device;

Academy Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the Academy community is not allowed;

- Permission must be sought before any image or sound recordings are made on the devices of any member of the Academy community;

- Where the Academy provides mobile technologies such as phones, laptops

and PDAs for offsite visits and trips, only these devices should be used;

- Where the Academy provides a laptop for staff, only this device may be used to conduct Academy business outside of Academy.

20.4 Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please ensure the following guidelines are adhered to:

- Only use recommended removable media;
- Store all removable media securely;
- Removable media must be disposed of securely by your ICT support team.

21.0 Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software;

- Always keep servers in a locked and secure environment;

- Limit access rights to ensure the integrity of the standard build;

- Always password protect and lock the server;

- Existing servers should have security software installed appropriate to the machine's specification;

- Back up tapes should be encrypted by appropriate software;

- Data must be backed up regularly;

- Back up tapes/discs must be securely stored in a fireproof container;

- Back up media stored off-site must be secure;

- Remote back ups should be automatically securely encrypted;

- Regular updates of anti-virus and anti-spyware should be applied;

- Records should be kept of when and which patches have been applied;

- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength.

22.0 Systems and Access

- You are responsible for all activity on Academy systems carried out under any access/account rights assigned to you, whether accessed via Academy ICT equipment or your own PC;

- Do not allow any unauthorised person to use Academy ICT facilities and services that have been provided to you;

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else;

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information;

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access;

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time;

- Do not introduce or propagate viruses;

- It is imperative that you do not access, load, store, post or send from Academy ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Academy or may bring the Academy into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the Academy's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act);

- Any information held on Academy systems, hardware or used in relation to Academy business may be subject to The Freedom of Information Act;

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998;

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing of the data.

23.0 Telephone Services

You may make or receive personal telephone calls provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others;

- They are not for profit or to premium rate services;

- They conform to this and other relevant Academy policies.

23.1 Mobile Phones

- You are responsible for the security of your Academy mobile phone. Always set the PIN code on your Academy mobile phone and do not leave it unattended and on display (especially in vehicles);

- Report the loss or theft of any Academy mobile phone equipment immediately;

- The Academy remains responsible for all call costs until the phone is reported lost or stolen;

- You must read and understand the user instructions and safety points relating to the use of your Academy mobile phone prior to using it;

- Academy SIM cards must only be used in Academy provided mobile phones;

- All Academy mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default;

- You must not send text messages to premium rate services;

- In accordance with the Finance policy on the private use of Academy provided mobiles, you must reimburse the Academy for the cost of any personal use of your Academy mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator;

- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.