



E Safety, Data Safety and ICT Usage Policy

Version	Date of Issue	Authorised by	Review Date
1	June 2010	Academy Governing Body	June 2011

CONTENTS

INTRODUCTION	3
MONITORING	4
BREACHES.....	4
INCIDENT REPORTING	5
ACCEPTABLE USE AGREEMENT: STUDENTS	6
ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS	8
COMPUTER VIRUSES	9
DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY.....	9
EMAIL	10
MANAGING EMAIL	10
SENDING EMAILS	11
RECEIVING EMAILS	11
EMAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION	11
EQUAL OPPORTUNITIES.....	12
STUDENTS WITH ADDITIONAL NEEDS	12
E-SAFETY	10ERROR! BOOKMARK NOT DEFINED.
E-SAFETY - ROLES AND RESPONSIBILITIES	12
E-SAFETY IN THE CURRICULUM	12
E-SAFETY SKILLS DEVELOPMENT FOR STAFF	13
MANAGING THE ACADEMY E-SAFETY MESSAGES	13
INCIDENT REPORTING, E-SAFETY INCIDENT LOG & INFRINGEMENTS	13
INCIDENT REPORTING	13
INTERNET ACCESS	12
MANAGING THE INTERNET	13
INTERNET USE	14
PASSWORDS AND PASSWORD SECURITY	15
PASSWORDS	15
PASSWORD SECURITY	15
REMOTE ACCESS	15
AUTHORISED SIMS LEARNING GATEWAY (SLG) USERS.....	15
ACCEPTABLE USE.....	154
PASSWORDS	155

SAFE USE OF IMAGES	165
TAKING OF IMAGES AND FILM.....	17
CONSENT OF ADULTS WHO WORK AT THE ACADEMY.....	17
PUBLISHING STUDENT’S IMAGES AND WORK.....	17
CCTV.....	18
VIDEO CONFERENCING	18
ICT EQUIPMENT & REMOVABLE MEDIA	18
ACADEMY ICT EQUIPMENT.....	18
PORTABLE & MOBILE ICT EQUIPMENT.....	19
PERSONAL PORTABLE DEVICES (INCUDING PHONES).....	19
ACADEMY PROVIDED PORTABLE DEVICES (INCLUDING PHONES).....	20
SYSTEMS AND ACCESS.....	20
TELEPHONE SERVICES	21
ACADEMY MOBILE PHONES	21
FURTHER HELP AND SUPPORT	21
ACKNOWLEDGEMENTS.....	22
CURRENT LEGISLATION.....	22
ACTS RELATING TO MONITORING OF STAFF EMAIL.....	22
OTHER ACTS RELATING TO E-SAFETY.....	22
ACTS RELATING TO THE PROTECTION OF PERSONAL DATA.....	24

Introduction

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

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Francis Combe Academy, we understand the responsibility to educate our students on e-safety issues, teaching them the appropriate behaviours and critical thinking skills needed for them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Academies hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the Academy. This can make it more difficult for your Academy to use technology to benefit learners.

Everybody in the Academy has a shared responsibility to secure any sensitive information used in their day to day professional duties, and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

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 computers, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc) and technologies owned by students and staff, but brought onto the Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the Academy at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, 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.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

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.

Breaches

A breach or suspected breach of policy by an Academy employee, contractor or student 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.

The Information Commissioner's Office's new powers to issue monetary penalties came into force on 6 April 2010, allowing the ICO to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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 Academy's Principal, Vice Principal or ICT Manager.

Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported Line Manager or Principal.

Acceptable Use Agreement: Students

Student Acceptable Use Agreement and E-safety Rules

- I will only use Academy ICT systems, including the Internet, email, digital video, and mobile technologies, for Academy purposes.
- I will not download or install software on the Academy's equipment.
- I will only log on to the Academy network and VLE, or any online services such as Google, with my own user name and password.
- I will not give permission to anyone else to use any of my accounts.
- I will follow the Academy's ICT security system and not reveal my passwords to anyone, and I will change them regularly.
- I will only use my Academy email 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 browse, download, upload or forward material that could be considered offensive or illegal. If I 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, nor that of anyone else.
- 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 will not be distributed outside of the Academy without the permission of the Principal or Vice Principal.
- I will ensure that my online activity, both inside and outside of the Academy, will not cause distress to my Academy, the staff, students or others, nor bring them into disrepute.
- I will respect the privacy and ownership of others' work 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 that this log 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.



Dear Parent/ Carer

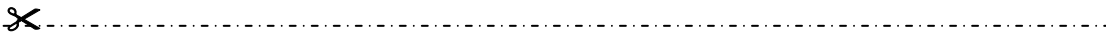
Information and Communications Technologies, including the Internet, Virtual Learning Environments, email and all types of computer, have become an important part of learning in our Academy. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of e-safety 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 problems can be discussed with their class teacher or the Academy e-safety Coordinator (Vice Principal).

Please return the bottom section of this form to Academy for filing.

Yours faithfully,

Principal



Student and Parent/ carer signature

We have discussed this document and(student name) agrees to follow the e-safety rules, and to support the safe and responsible use of ICT at Francis Combe Academy.

Parent/ Carer Signature

Student Signature.....

Form Date

Acceptable Use Agreement: Staff, Governors and Visitors



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

Information and Communications Technologies, including email, the Internet, Virtual Learning Environment, and all types of computer, are an expected part of our daily working life in 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 Principal or Vice Principal.

- I will only use the Academy's email, Internet connection, 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 not allow any other individual to use any of my system accounts (network, VLE etc.)
- I will ensure that all electronic communications are compatible with my professional role.
- I will use only the approved, secure email system for Academy business.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will ensure that personal data (such as data held on SIMS or similar software) is kept secure and is used appropriately, whether in the 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. (For information on this, see the ICT Manager.)
- I will not install any hardware or software without permission of ICT Support.
- 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 in line with Academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside of 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 that this log 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 inside and outside of the 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.
- I understand this forms part of the terms and conditions set out in my contract of employment.

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)

Job title

Computer Viruses

Before use, all files downloaded from the Internet, received via email or carried on removable media (e.g. floppy disk, CD) are automatically checked for viruses with network software.

Never interfere with any anti-virus software installed on Academy ICT equipment that you use. If your machine is not routinely connected to the Academy network, you must make provision for regular anti-virus updates through ICT Support.

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

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency or via the Hertfordshire Business Services (HBS) disposal scheme. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

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

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-agency.gov.uk/business/topics/waste/32084.aspx>

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

The Academy maintains a comprehensive inventory of all its ICT equipment including a record of disposal. The Academy's disposal record will include:

- Date item is disposed of
- Authorisation for disposal, including:
 - verification of software licensing
 - details of personal data likely to be held on the storage media
- How it was disposed of eg waste, gift, sale
- Name of person and/or organisation who received the discarded item
- 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

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/computers/pc_disposal.shtml

EMAIL

Managing email

The Academy gives all staff their own email account to use for all Academy business. This is to minimise the risk of them receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. The Academy email account should be the account that is used for all Academy business.

Under no circumstances should staff conduct any Academy business using personal email addresses.

The Academy requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the Academy or the LA'. The responsibility for adding this disclaimer lies with the account holder.

All emails should be written and checked carefully before sending, in the same way as a letter written on Academy headed paper.

Staff sending emails to external organisations, parents or students are advised to cc. the Principal or line manager.

Emails created or received as part of your Academy job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

- Delete all emails of short-term value
- Organise email into folders and carry out frequent house-keeping on all folders and archives

- The forwarding of chain letters is not permitted in the Academy.
- All student email users are expected to adhere to the generally accepted rules of e-safety and netiquette.
- Students must immediately tell a teacher or other trusted adult if they receive an offensive email.
- Staff must inform their line manager or the E-safety Co-ordinator if they receive an offensive email.
- However you access your Academy email (whether directly, through webmail when away from the office or on non-Academy hardware) all of the Academy email policies apply.
- It is not permitted to use any web based email service for sending, reading or receiving business related email.

Sending emails

When sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section entitled “Emailing Personal, Sensitive, confidential or Classified Information.”

An outgoing email greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming email. Whenever possible, send the location path to the shared drive rather than sending large attachments

Receiving emails

- Check your email at least once a day.
- Activate your ‘out-of-office’ notification when away for extended periods.
- Never open attachments from an untrusted source. Consult ICT Support first.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

Emailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data is not recommended and should be avoided where possible.

It is not permitted to use any web based email service for sending email containing sensitive information.

- Where your conclusion is that email must be used to transmit such data, obtain the express consent of your manager to proceed.
- Exercise caution when sending the email, and always follow these checks before releasing the email:
- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email to any more recipients than is absolutely necessary
- Do not send the information to anybody whose details you have been unable to verify (usually by phone)
- Send the information as an encrypted document **attached** to an email
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

When sending an email containing personal or sensitive data you need to put a security classification in the first line of the email. For emails to do with information about a student, for example, you need to put in **PROTECT – PERSONAL** on the first line of the email.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Students with Additional Needs

Some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

E-safety

E-safety - Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the Academy, the Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in this Academy is the Vice Principal Extended Academy 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 E-safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Principal or E-safety 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 and Student Discipline (including the anti-bullying) policy, and PSHE.

E-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the students on a regular and meaningful basis.

Students should be made aware of the relevant legislation when using the Internet such as those regarding data protection and intellectual property, which may limit what they want to do, but also serves to protect them.

Students are aware of the impact of cyberbullying, and know how to seek help if they are affected by any of its forms. 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 or carer, teacher or other trusted staff member, an organisation such as Childline, or by the use of the CEOP "report abuse" button

Students are taught to evaluate websites critically, and learn good search skills via the ICT curriculum, with specific lessons in Years 7 and 8.

e-safety Skills Development for Staff

New staff receive information on the Academy's acceptable use policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of young people within the context of e-safety and know what to do in the event of misuse of technology by any member of the Academy community. .

Managing Academy E-safety Messages

We endeavour to embed e-safety messages across the curriculum whenever the Internet or related technologies are used.

The e-safety policy will be introduced to the students at the start of each Academy year, and e-safety posters will be prominently displayed throughout the Academy.

Incident Reporting, E-safety Incident Log & Infringements

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 Academy's SIRO or e-safety Co-ordinator.

Additionally, all security breaches, lost or stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance, must be reported to your Senior Information Risk Owner.

Internet Access

Managing the Internet

Academy students have access to the Internet through the Academy's Internet connection.

Staff will preview any recommended sites before use.

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 copyright of materials from all sources.

Internet Use

- Users must not post personal, sensitive, confidential or classified information, or disseminate such information in any way that may compromise recipients, the data subject or the user.
- Do not reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed
- 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, and the incident reported immediately to the E-safety Co-ordinator or teacher as appropriate.
- It is the responsibility of the Academy, by delegation to the ICT Manager, to ensure that Anti-virus software 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 the ICT Manager's to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the 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 Principal or ICT subject leader
- If there are any issues related to viruses or anti-virus software, the ICT Manager should be informed.

At present, the Academy endeavours 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 and home phone numbers, Academy details, IM identities or email address).

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.

The Academy disseminates information to parents relating to e-safety where appropriate in the form of;

- Information and celebration evenings
- Posters
- Website and VLE postings
- Newsletter items
- VLE training

Passwords and Password Security

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 and students 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.

Passwords must contain a minimum of six characters and be difficult to guess.

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

Password Security

Password security is essential for staff, particularly as they are able to access and use student 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 and SIMS log-in username (where appropriate).

Staff are aware of their individual responsibilities to protect the security and confidentiality of the Academy network, SIMS and VLE, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unlocked.

Remote Access

Users are responsible for all activity via their remote access facility.

Only use equipment with an appropriate level of security for remote access.

To prevent unauthorised access to Academy systems, keep all access information such as logon IDs and PINs confidential, and do not disclose them to anyone.

Select PINs and passwords to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers.

Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Protect Academy information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from outside of the Academy.

Authorised SIMS Learning Gateway (SLG) Users

- Access to the FCA SLG system is provided only to the persons who are legally responsible for pupil(s) currently attending FCA.
- Access to SLG will only be granted on condition that the individual formally agrees to the terms of this policy by returning a parent access request form.
- Authorising members of Academy staff must confirm that there is a legitimate entitlement to access pupil(s) information.

Acceptable use

- Users must not distribute or disclose any information obtained from the SLG to any person(s) with exception of the pupil(s) to which the information relates to or other adults with parental responsibility.
- Do not access the SLG in an environment where security of the information may be at risk e.g. cybercafé.
- Ensure that you log out of the SLG when leaving your computer for a period of time.
- Do not post offensive, libellous, defamatory, intimidating, misleading or disruptive comments to the Academy or bring the Academy disrepute.

Password

- Users assume personal responsibility for your username and password.
- Do not use or share anyone else's username and password to access the academy SLG.
- Users must keep username and password confidential.
- Users must change the password when ever prompted by FCA SLG.
- Password must be at least 7 characters in length.
- Passwords must contain at least 1 number (0-9), one upper case and one lower case alphabetical character and one symbol e.g. #%\$£!

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, to 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 of taking the pictures.

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

Neither students nor staff are permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, including 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 device on which they were captured.

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 copies are located in personnel files

Publishing Students' Images and Work

On a child's entry to the Academy, all parents and 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 VLE
- in the Academy prospectus and other printed publications which the Academy may produce for promotional purposes
- recorded or transmitted on a camcorder, digital camera 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, ie an exhibition promoting the Academy
- general media appearances, eg local or national media or press releases 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 and carers may withdraw permission, in writing, at any time.

Students' names will not be published alongside their image. Email 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.

Only designated personnel have authority to upload to the website.

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 http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

Video Conferencing

Permission is sought from parents and carers if their young people are involved in video conferences

All students are supervised by a member of staff when video conferencing

The Academy keeps a record of video conferences, including date, time and participants.

Approval of the Principal is sought prior to all video conferences within the Academy

The Academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

No part of any video conference is recorded in any medium without the written consent of those taking part

Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see

<http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml>Academy ICT

ICT Equipment & Removable Media

Academy ICT Equipment

Users of ICT are responsible for any activity undertaken with the Academy's ICT equipment provided to them

The Academy logs all ICT equipment issued to staff, and serial numbers are recorded as part of the Academy's inventory

Users should not allow 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.

Users must ensure that all ICT equipment they use is kept physically secure.

Users must 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 users save data on a frequent basis to the Academy's network drive. Users are responsible for the backup and restoration of any data that is not held on the Academy's network drive.

Confidential or sensitive data should not be stored on the local drives of desktop computers. 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 computers accessing personal data must have a locking screensaver.

Privately owned ICT equipment should not be used on the Academy network.

On termination of employment, users must return all ICT equipment to the ICT Manager.

It is the responsibility of users to ensure that any information accessed from their computer or removable media equipment is kept secure, and that no sensitive, confidential or classified information is disclosed to any unauthorised person

All ICT equipment allocated to staff must be authorised by the ICT Manager.

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

Portable & Mobile ICT Equipment

This section covers such items as laptop computers, PDAs and removable data storage devices, henceforth referred to as “portable 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 will be monitored in accordance with the general policy.

Staff must ensure that all Academy data is stored on the Academy’s network, and not kept solely on the portable device. Any confidential data stored on such devices must be encrypted.

Equipment must be kept physically secure in accordance with this policy in order to be covered for insurance purposes. When travelling by car, best practice is to place the portable device 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 devices are 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 ICT Support.

In areas where there are likely to be members of the general public, portable devices must not be left unattended, and must be kept out of sight.

Portable devices must be transported in their protective cases if supplied.

Personal Portable Devices (including phones)

The Academy allows staff and students to bring in personal mobile phones and other portable devices for their own use. Under no circumstances does the Academy allow a member of staff to contact a student,

parent or carer using their personal device. Nor may they be used for any personal reason during lesson time, and they must be switched to silent mode at those times.

Students are also allowed to bring personal portable devices to the Academy. However, they may not be used for any personal reason during lesson time, and they must be switched to silent mode at those times.

These technologies may be used, however for educational purposes, as mutually agreed with the Principal. The device user, in this instance, must always seek 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 members 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 Portable Devices (including phones)

The sending of inappropriate text messages between any members of the Academy community is not allowed.

Permission must be sought before any image or sound recordings are made 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.

Systems and Access

Users are responsible for all activity on Academy systems carried out under any access or account rights assigned to them, whether accessed via Academy ICT equipment or their own computer

- Do not allow any unauthorised person to use Academy ICT facilities and services that have been provided to you
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure that you logoff from the computer completely when you are going to be away from the computer for a longer period of time
- 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, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Academy or may bring the Academy or HCC 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

Telephone Services

Users 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 HCC and Academy policies.
- Academy telephones are provided specifically for Academy business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

Academy 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
- Report the loss or theft of any Academy mobile phone 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. Payment arrangements should be made through the Finance Department
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 emergency calls may be made if it would be unsafe to stop before doing so

Further help and support

Francis Combe Academy has a legal obligation to protect sensitive information under the Data Protection Act 1998. For more information visit the website of the [Information Commissioners Office](http://www.ico.gov.uk/) [<http://www.ico.gov.uk/>].

Advice on e-safety - <http://www.thegrid.org.uk/eservices/safety/policies.shtml>

Further guidance - <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

School's toolkit is available - Record Management Society website – <http://www.rms-gb.org.uk/resources/848>

Test your online safety skills [<http://www.getsafeonline.org>]

Acknowledgements

SSE, CSF, ICT Team

Becta

Cabinet Office

Information Commissioners Office

LGFL

Thomas Coram Academy

Record Management Society

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmsso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000

<http://www.hmsso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to Academy activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmsso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>

Other Acts Relating to E-safety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Academics should already have a copy of “*Young people & Families: Safer from Sexual Crime*” document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person’s password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone’s work without obtaining their author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Young people Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of young people in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx