CA/15/1/14

ESAFETY, DATA SECURITY AND ACCEPTABLE ICT USE POLICY

Approved by Governors	25 March 2015
Review Date	Spring 2017

Preface to all policies and procedures.

Colchester Academy aims to be the first choice provider of outstanding learning for the community of Colchester and beyond. The Academy will provide exciting and challenging academic, vocational and social learning opportunities locally, nationally and internationally. The Academy will prepare students for a rapidly changing world and nurture a philosophy of lifelong learning that they will maintain into adulthood. All students and staff will be nurtured, motivated and encouraged to be the best they can be.

Colchester Academy's ethos is founded on a set of key principles which will inspire and be evident in all the Academy does. These principles are:

- Harnessing the specialisms of English and Health Sciences
- A culture of high aspirations, high achievement and success for all
- Respect for others and self, with all people feeling valued
- A secure and healthy environment which is at the heart of the community.

This policy is based on the Essex County Council eSafety and Data Security Guidance Policies for Acceptable ICT Use.

CONTENTS

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

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
- 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/ or 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 Colchester 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.

Schools 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 the 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 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).

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 emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) of all users of the Academy's ICT systems (including students, staff, governors and 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 Staff Disciplinary (Misconduct) Procedure.

Policy breaches may also lead to criminal or civil proceedings.

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 Finance and Operations Director 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 to the ICT Manager.

See flowcharts on page 17 for dealing with both illegal and non-illegal incidents

Colchester Academy

Acceptable Use Agreement: Students

Student Acceptable Use - Agreement / eSafety Rules

- I will only use ICT systems in the Academy, including the internet, email, 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/ Learning Platform 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 email address.
- I will make sure that all ICT communications with students, teachers or others are 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 Principal/Associate Principal.
- I will ensure that my online activity, both in Academy and outside Academy, will not cause my 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 or any other Academy security 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.

Dear Parent/ Carer

ICT including the internet, learning platforms, email 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 form tutor, Year Leader or ICT teacher.

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

This Acceptable Use Agreement is a summary of our eSafety, Data Security and Acceptable ICT Use Policy which is available in full on our website.

Yours sincerely

✂----------

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 Colchester Academy.

Parent/ Carer Signature ……..……..……

Student Signature…….

Form …… Date ……

Colchester Academy

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 email, the internet and mobile devices 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 Finance and Operations Director or ICT Manager.

- I will only use the Academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal 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 email address and social networking identities to students.
- I will only use the approved, secure email 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 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 or software without permission of the ICT 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 in line with Academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Academy network without the permission of the parent/ carer and Principal/Associate Principal.
- I understand that all my use of the Internet, communication and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal/Associate Principal.

- I understand that during my absence from work ICT authorised staff may, without prior notice, access my email or voicemail account where applicable, in order to deal with any business-related issues retained on that account.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in and outside Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's e-Safety, Data Security and Acceptable ICT Use Policy and help students to be safe and responsible in their use of ICT and related technologies.
- I will ensure that when saving data on system either locally or remotely that it is stored in a location with appropriate security applied

This Acceptable Use Agreement is a summary of our eSafety, Data Security and Acceptable ICT Use Policy which is available in full on the Academy Staff Shared Area and website.

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/Role . . . . . .

Computer Viruses

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

- 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 virus updates through the ICT team

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

Email

The use of email within most schools is an essential means of communication for both staff and students. In the context of Colchester Academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, students must have experienced sending and receiving emails.

Managing email

- The Academy gives all staff their own email account to use for all Academy business as a work based tool. This is to minimise the risk of 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 the 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 sole account that is used for all Academy business

- Under no circumstances should staff contact students, parents or conduct any Academy business using personal email addresses

- The Academy attaches a standard disclaimer to all email correspondence sent externally to the Academy, stating that, 'the views expressed are not necessarily those of the Academy'

- All emails should be checked carefully before sending including the intended recipients

- Staff sending emails to external organisations, parents or students are advised to cc. the line manager or appropriate member of SLT

- Students may only use Academy approved accounts on the Academy system and for educational purposes

- Emails created or received as part of your Academy role 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 Academy.

- All student email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission from Principal

- Students must immediately tell a teacher/trusted adult if they receive an offensive email

- Staff must inform the ICT Manager if they receive an offensive email

- Students are introduced to email as part of the ICT Scheme of Work and Personal Guided Learning Time

- However you access your Academy email (whether directly, through webmail when away from the Academy or on non-Academy hardware) all the Academy email policies apply.

- When accessing email remotely on non-Academy equipment staff must take care to ensure that they correctly log out of the session and that passwords are not cached (stored) on the device.

- Email pertaining to Colchester Academy business either directly or indirectly should not be sent or received through non-Colchester Academy email addresses personal email addresses

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section of this policy about Emailing Personal, Sensitive, Confidential or Classified Information

- Use your own Academy email account so that you are clearly identified as the originator of a message

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily.

- An outgoing email greater than twenty-five megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming email. The recipients email system may however have lower limits.

- Academy email is not to be used for personal advertising

Receiving emails

- Check your email regularly

- Activate your 'out-of-office' notification when away for extended periods
- Use the 'Delegation' facility within your email software so that your email can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; consult the ICT Services Teamfirst.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder/data store
- The automatic forwarding and deletion of emails is not allowed

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 wherever possible. If confidential information is required to be sent the information should be sent as an encrypted attachment and the password disclosed to the recipient by another method (eg telephone). This also extends to sensitive and confidential data sent by post.
- Confidential or other sensitive data relating to Colchester Academy either directly or indirectly must not be sent to or from a webmail account (for example, but not limited to Gmail, Hotmail or BTInternet) with the exception of an Colchester Academy Office 365 account which uses secure connections authenticated by a Colchester Academy managed account
- Where your conclusion is that email must be used to transmit such data:

  - Obtain express consent from the relevant member of SLT to provide the information by email
  - 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/person whose details you have been unable to separately 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) – preferably by telephone
  - Do not identify such information in the subject line of any email
  - Request confirmation of safe receipt

Equal Opportunities

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.

eSafety

eSafety - Roles and Responsibilities

As eSafety 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 Academy's eSafety co-ordinator is the Assistant Principal in charge of eSafety 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 ECC, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior staff 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, Rewards and Sanctions and Anti-Bullying policies and PSHE

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 has a framework for teaching internet skills in ICT lessons.
- 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

- 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 (a link to CEOP can be found on the Academy website)

- Students are taught to critically evaluate materials and learn good searching skills through the curriculum including ICT lessons) and discussions in Personal Guided Learning Time

eSafety Skills Development for Staff

- Our staff receive regular information on eSafety issues

- New staff receive information on the Academy's eSafety, Data Security and Acceptable ICT Use Policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the Academy community (see enclosed flowchart)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

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

Incident Reporting, eSafety 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 ICT Manager or eSafety Co-ordinator. 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 to the Finance and Operations Director or ICT Manager

eSafety Incident Log

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

COLCHESTER ACADEMY
e-Safety Incident Log

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

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Principal/Associate Principal. Incidents should be logged and the **Essex Flowcharts for Managing an eSafety Incident** should be followed.

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 (see flowchart)

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Has illegal activity taken place?

Still unsure?

For further advice ECC ISIS helpdesk on

Examples of illegal activity would include:

- Downloading abusive images
- Passing child pornography to

YES

- ✓ Inform Essex Police and Essex County Council
- ✓ Follow the advice given by the Police, or
- ✓ Confiscate the device and if related to the Academy network disable user account
- ✓ Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

NO

Go to next flowchart which outlines the process for non-illegal incidents

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place

The Headteacher/e-Safety Co-ordinator should:

- **Record the incident in the e-safety log**

Did the incident involve a member of staff?

YES

If a member of staff has:

1. Behaved in a way that has, or may have, harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children Contact LADO on 01245 436744

- Review evidence and determine whether the incident was accidental or deliberate

NO

Was the Child the victim or perpetrator

Pupil as Victim

Support the pupil by one or more of the following:

- Class Teacher
- e-Safety Co-ordinator
- Headteacher/Senior Leader

Pupil as Instigator

Incident types could be:

- Using another persons user name or password
- Accessing websites which are against the Academy's policy e.g. gaming
- Using a mobile

- Review incident to decide if other students were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident

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. All use of the internet in the Academy is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Academy students 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.
- 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

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, 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

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

Infrastucture

- Colchester Academy employs web filtering which is the responsibility of the ICT Manager
- Colchester 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 ICT manager, 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 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 ICT Manager/Technician 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 ICT Manager

- If there are any issues related to viruses or anti-virus software, the ICT Manager should be informed

Managing Other Web 2.0 Technologies

Web 2.0, including social networking sites, blogs and wikis, 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 2.0 spaces in order to communicate with students using the Academy Learning Platform or other systems approved by the

Principal

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 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 and students are actively encouraged to contribute to adjustments or reviews of the Academy eSafety, Data Security and Acceptable ICT Use policy through the Parents' Forum
- 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)
- The Academy disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform 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 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 meet Academy requirements

- User ID and passwords for staff and students who have left the Academy are removed from the system within one week

If you think your password may have been compromised or someone else has become aware of your password report this to the ICT Services team as soon as possible.

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

- Students are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. From Year 7 they are also expected to use a personal password and keep it private

- Students are not allowed to deliberately access on-line materials or files on the Academy network, of their peers, teachers or others unless working collaboratively.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of Academy networks, MIS systems and/or Learning Platform, 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.

Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the Academy and therefore no longer have authorised access to the Academy's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the Academy has left

- Prompt action on disabling accounts will prevent unauthorized access

Generic Accounts

The use of generic or shared accounts is not encouraged and is to be avoided where possible. Where this cannot be avoided the accounts should be setup so they cannot be logged on to or the password changed on a regular basis (industry standards advise every 42 days)

Personal or Sensitive Information

Protecting Personal, 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 or organization.

- 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 Multi-Function Device (MFD) (print, fax, scan and copy devices) 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 policy

- It is the responsibility of the member of staff saving data on system to ensure that it is stored in a location with appropriate security applied – if you are unsure about the security applied to any particular location the IT Services team will be able to advise you on the access available to any specific location.

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

- Ensure removable media is purchased with encryption

- Store all removable media securely in a locked cabinet or cupboard

- Securely dispose of removable media that may hold personal data in such a way that it cannot be recovered (simply deleting data is not sufficient)

- 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 in such a way that it cannot be recovered (simply deleting data is not sufficient)

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Cloud and other Remote Storage Services.

- Data regarding Colchester Academy should only be stored in the Colchester Academy domain (either on site or in the Colchester Academy Office 365 environment). Services such as Dropbox or other file/data hosting should not be used to store or transfer Colchester Academy data.

- It is the responsibility of the member of staff saving data to ensure that it is stored in a location with appropriate security applied – if you are unsure about the security applied to any particular location the IT Services team will be able to advise you on the access available to any specific location.

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to Academy systems, keep all remote access information such as logon IDs and Passwords confidential and do not disclose them to anyone
- Select Passwords and PINs 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 a non-Academy environment

Safe Use of Images

Taking of 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. ECC guidance can be found at: http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc

- 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 in a shared location and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of other students (or staff), 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 pupil's device

Publishing Students' Images and Work

On a student'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/Learning Platform
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes
- in the Academy Newsletter
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- parents are asked to give permission for their child's name to be used

This consent form is considered valid for the entire period that the student attends the Academy unless there is a change in the student'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.

Storage of Images

- Images/ films of students 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 Academy staff and students as appropriate within the confines of the Academy network/ Learning Platform
- the ICT Manager has the responsibility of archiving and deleting the images when they are no longer required, or the student has left the Academy

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

Academy ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the Academy's ICT equipment provided to you
- ICT equipment issued to staff will be recorded including the 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 in a locked cupboard or cabinet
- 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 or laptops. 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 must 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)

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

- Equipment must not be left in any unattended vehicle at any time

- Synchronise all locally stored data, with the central Academy network server or Colchester Academy One Drive storage 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, wherever possible, must be kept out of sight and secured with a lock where appropriate

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

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.

Monitoring, Evaluation and Review

The Governing Body will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Academy