Enterprise South Liverpool Academy

E-Safety

The sponsors' mission is that the Enterprise South Liverpool Academy (ESLA) equips all members of its learning community with the values, skills and attributes they will need for personal success and well-being in a multi-cultural society and global economy

Also to significantly contribute to community cohesion and regeneration as a centre of learning to provide support, training and business opportunities for the benefit of all local people.

*The **Enjoyment of Learning**, the opportunities provided through the **Enterprise and Business** and **Languages for Business** specialisms and a culture that reflects **Christian Values and Principles** are the core characteristics of the Academy. These complementary core elements are evident in everything the Academy does and represents.*

APPROVED DATE	Pending - Governors		
REVIEW DATE	December 2015		
SIGNED HEAD OF SCHOOL	K. Unsworth	PRINT NAME	KEVIN UNSWORTH
SIGNED CHAIR OF GOVERNORS		PRINT NAME	KEITH SEXTON

Introduction

The purpose of this e-safety policy is to outline what measures the academy takes to ensure that students and staff can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion. It aims to provide clear advice and guidance on how to minimise risks and deal with any infringements.

Although devices, forms of cyber-misuse, internet and social networking sites specified in this policy may be referred to by brand name for quickness of communication and ease of understanding, the policy should be understood as being agnostic with regard to brand and applicable to equivalent devices, websites, or forms of misuse regardless of manufacturer, internet services provider, or minor variation in misuse strategy

Roles and Responsibilities

Within the academy all members of staff and students are responsible for e-safety, responsibilities for each group include:

Students

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.
- Compliance with the Student's Acceptable Use Policy (AUP) to which students must agree prior to use of academy ICT equipment either in the academy or remotely.
- Reporting any e-safety issue to the teacher, team leader or parent.
- Take responsibility for their own actions using the internet and communications technologies.

Parents/Carers

- Providing consent for their child to use the Internet and other ICT technologies as an integral part of the Student's Acceptable Use Policy (AUP) form at the time of entry into the Academy.
- Supporting the Academy in its eSafety activities by reinforcing acceptable use and e-behaviour messages

Staff

- Having a clear understanding of e-safety issues and the required actions including
    - Safe use of e-mail;
    - Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
    - Safe use of Academy network, equipment and data;
    - Safe use of digital images and digital technologies, such as mobile phones and digital
    - cameras;
    - Publication of student information/photographs and use of website;
    - eBullying / Cyberbullying procedures;
    - Their role in providing e-Safety education for students;
- Reporting any e-safety issues to the ICT Manager as soon as the issue is detected.
- Compliance with the Staff Acceptable Use Policy (AUP) to which staff must agree prior to use of academy ICT equipment either in the academy or remotely.
- Educating students on e-safety and re-enforcing this in the day to day use of ICT in the classroom
- Fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials

ICT Manager

- Keeping up to date with e-Safety issues and guidance through liaison with the relevant organisations
- Updating the principal, governors and senior management on e-Safety; providing information and instruction on an annual basis on policy developments, issues and strategies
- Referring any material believed to be suspect to the appropriate authorities e.g. Careline, police.
- Ensuring that the best technological solutions are in place to ensure e-safety whilst still enabling students to use the internet effectively in their learning.
- Ensuring that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.
- Checking and auditing all systems to ensure that no inappropriate data is stored or is accessible.
- Working with the Safeguarding team to create, review and advise on e-safety and acceptable use policies.

Governors and Academy Senior Leadership

- Embedding safe practices into the culture of the Academy
- Ensuring this policy is implemented and compliance is monitored.

Policy

It is the duty of the Academy to ensure that every student in their care is safe. This applies equally to the virtual or digital environment as it does to the physical environment. The academy therefore endeavours to ensure the e-safety of all academy members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this. Current and emerging technologies used in ESLA and, more importantly in many cases, used outside of the Academy by students include:

- Internet
- e-mail
- Instant messaging (often using web cams)
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites (Skype)
- Chat Rooms
- Gaming Sites
- Music/Video download sites (Youtube/Spotify)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down ‘Office’ applications.
- Games consoles with chat and video capabilities (xbox live/Playstation Network)

The Academy will therefore, as far as reasonably practicable, ensure that these technologies are safe for students and staff to use by deploying the following approaches.

Internet

- Maintain broadband connectivity through an accredited supplier
- Work in partnership with the supplier to ensure any concerns about the system are communicated to the supplier so that systems remain robust and protect students;
- Ensure network health through appropriate anti-virus software etc. and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc.;
- Ensure their network is ‘healthy’ by having the Academy ICT technical team carry out regular audits.
- Utilise 'e-safe' forensics software externally monitored by CEOP trained forensic experts
- Ensure the ICT Manager is up-to-date with the suppliers services and policies;

- Ensure the ICT Manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allow students access to Internet logs;
- Use individual log-ins for students and all other users;
- Use teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never send personal data over the Internet unless it is encrypted or otherwise secured;
- Ensure students only publish within appropriately secure learning environments
- Used internal filtering system alongside the 'e-safe' and supplier filtering systems which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature
- Use an industry recognised Hardware firewall to protect staff and students from external threats

With specific reference to publishing information on the ESLA website,

- Only the ICT team will be granted rights to upload information and therefore have overall technical responsibility for the site
- Only excerpts will be published from student's work and all work will be checked to ensure no reference is made to named individuals, no infringements of copyright or other relevant legislation has occurred and, where applicable, appropriate credits has been given to information sources; editorial responsibility therefore lies with the member of staff submitting the work for publication.
- All links will be checked for suitability at the time of linkage and periodically after this to ensure continued suitability

Email

- Email will be restricted to approved addresses and filtered for unsuitable content and virus
- In the Academy context, e-mail will not be considered private and the Academy reserves the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.
- The use of personal e-mail addresses, such as Hotmail, will be avoided by all staff and staff should use the Academy's systems wherever possible for professional purposes only.

Blogs, Chat Rooms, Podcasts and Social Network Sites

All sites are blocked except those that are part of an educational network or approved learning platform.

Music Download, Gaming and Shopping Sites

These sites are blocked within the Academy
.

Webcams and Video Conferencing

Only approved video conferencing system services will be used. Only approved or checked webcam sites will be used.

Mobile and Smart Phones

The Academy will require all mobile and smart phones to be used in line with its communications and behaviour for learning policies. In addition to the above, e-Safety will be thematic throughout the curriculum. In relation to teaching and learning, staff will

- Supervise students at all times, as far as reasonably practicable, and will be vigilant in learning resources areas where older students have more flexible access.
- Plan the curriculum and internet use to match students' abilities
- Be vigilant when conducting raw image searches with students

Staff will ensure that students

- Know what to do if they find inappropriate web material i.e. to switch off monitor close the laptop and report the URL to the teacher or ICT Manager.

- Know what to do if there is a cyber-bullying incident;
- Have a clear, progressive e-safety education programme throughout all Key Stages, built on LA / national guidance. Students will be taught a range of skills and behaviours appropriate to their age and experience, such as to:

    - STOP and THINK before they CLICK
    - expect a wider range of content, both in level and in audience, than is found in the Academy library or on TV;
    - discriminate between fact, fiction and opinion;
    - develop a range of strategies to validate and verify information before accepting its accuracy;
    - skim and scan information;
    - be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - know search engines / websites that would bring effective results;
    - know how to narrow down or refine a search;
    - [for older students] understand how search engines work;
    - understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
    - not download any files – such as music files - without permission;
    - understand why they should not post or share details of their personal lives, contact information, daily routines, photos and videos;
    - have strategies for dealing with receipt of inappropriate materials.

- When copying materials from the web, understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Are made aware of the risks and issues associated with communicating though email and have strategies to deal with inappropriate emails.
- Have a good awareness of 'netiquette' and appropriate e-behaviour appropriate to their age.

The Academy will make training available annually to staff on e-safety and will issue staff with the "What to Do If" guidance (Appendix 1). In addition, the Academy will run a rolling programme of advice, guidance and training for parents, including:

- Information in safety leaflets; in Academy newsletters; on the Academy web site;
- Demonstrations, practical sessions held at Academy;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.
- Information on how to report abuse or bullying

The Academy will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an Academy computer or mobile device. Neither the Academy nor the network provider can accept liability for material accessed, or any consequences of Internet access. Where inappropriate use or infringement of policy is detected the Academy will review the event and, if appropriate, implement sanctions in line with the following

Students

Category A Infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups

Possible Sanctions: Academy Behaviour Policy Level 2 (applied as with any other classroom misbehaviour).

Category B Infringements

- Use of Filesharing software e.g. Bitorrent, Bitlord, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Possible Sanctions: Removal within classroom from ICT equipment, Directorate detention, teacher / directorate contacts home, teacher to inform ICT Manager to invoke possible removal of Internet access rights for a period.

Category C Infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or instant message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Possible Sanctions: Immediate remove (i.e. A4) referral to ICT Manager with possible removal of Internet and/or ICT access rights for a period, Learning Manager to contact parents.

Category D Infringements

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the Academy name into disrepute

Possible Sanctions – Referred to Principal /involvement of relevant pastoral leader/ internal seclusion / exclusion / removal of equipment / involvement of Safe Schools Police Officer.

Staff

Inappropriate use of the Academy ICT arrangements by staff is defined in the Communications Policy and may be dealt with under the Academy Disciplinary Policy

Complaints

The ICT Manager will act as the first point of contact for any complaint. Complaints against staff will be referred to the Principal. Complaints against students will be handled in accordance with Academy behaviour and child protection policies. With specific regard to cyber-bullying, the Academy will make clear that the use of the web, text messages, email, video or audio to bully another student of member of staff will not be tolerated. If a bullying incident, directed at a student, occurs using email or mobile phone technology either inside or outside of Academy time staff should

- Advise the child not to respond to the message
- Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the Academy's Safeguarding officer

The ICT Manager/Safeguarding Officer may decide to:

- Remove the device to a secure place to ensure that there is no further access
- Inform the sender's e-mail service provider

- Notify parents of the students involved
- Consider informing the police depending on the severity or repetitious nature of offence
- Involve the safe schools officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff, the Academy's ICT Manager will be informed who will:

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate

Records of complaints will be maintained in line with Academy behaviour management policies and staff disciplinary policies.

Disaster Recovery

All ICT data will be backed up on a regular basis and back up will be stored in a secure location to enable system rebuild following a critical incident. Full details of ICT disaster recovery can be found in the Emergency Planning & Business Continuity policy.

Definitions

CEOP	Child Exploitation and Online Protection

Appendices

Appendix 1	What To Do If
Appendix 2	12 Rules for Responsible ICT Use
ESLAF16	Acceptable Use (Staff)
ESLAF17	ICT Equipment Loan Form
ESLAF18	Acceptable Use (Students)

Append ix 1 ‘ WHAT DO WE DO IF? ’

An inappropriate website is accessed unintentionally in the Academy by a child.

- Play the situation down; don’t make it into a drama.
- Decide whether to report to the ICT Manager and decide whether to inform the safeguarding team of any students who viewed the site.
- Inform the ICT Manager and ensure the site is filtered.

An inappropriate website is accessed intentionally by a child.

- Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions
- Inform the ICT Manager and ensure the site is filtered if need be.

An adult uses Academy IT equipment inappropriately.

- Ensure you have a colleague with you; do not view the misuse alone.
- Report the misuse immediately to the Principal and ensure that there is no further access to the PC or laptop.

The Academy will then consider the following course of action:

- If the material is offensive but not illegal, the Academy may decide to:
  - Remove the PC to a secure place.
  - Instigate an audit of all ICT equipment by the Academy’s ICT Support Team to ensure there is no risk of pupils accessing inappropriate materials in the Academy.
  - Identify the precise details of the material.
  - Take appropriate disciplinary action. (contact Personnel/Human Resources)
  - Inform governors of the incident.
- In an extreme case where the material is of an illegal nature:
  - Remove the PC to a secure place and document what you have done.
  - Contact the local police and follow their advice.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of Academy time.

- Advise the child not to respond to the message.
- Refer to relevant policies including e-safety and anti-bullying and apply appropriate sanctions
- Secure and preserve any evidence.

Inform the safeguarding team who will then oversee the following course of action:

- Notify parents of the students involved.
- Inform local police if required.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Inform ICT Manager who will:
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child’s safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

- Report to and discuss with the named child protection officer in Academy **as soon as possible.**
- Advise the child on how to terminate the communication and save all evidence.

  - Inform the Academy safeguarding team who will then oversee the following course of action:
  - Contact CEOP http://www.ceop.gov.uk/
  - Consider the involvement of police and social services.

All of the above incidences must be reported immediately to the ICT Manager.
Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Appendix 2: 12 RULES FOR RESPONSIBLE ICT USE

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the Academy's computers for Academy work and homework.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. I will keep my login and password secret.
5. I will not bring files into Academy without permission.
6. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the Academy.
7. I will only e-mail people I know, or my teacher has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
11. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.