Policy Review

This policy will be reviewed in full annually
The policy was last reviewed and agreed by Adam Russell, Head of Quality on 7th August 2018
It is due for review in August 2019

Introduction

This E-Safety Policy applies to all members of the Academy, including learners, staff, visitors and contractors who have access to, and are users of ICT systems and resources both in and out of learning venues, e.g. internet, electronic communications, Virtual Learning Environment (VLE) or mobile devices.

E-safety informs the wider safeguarding agenda and this policy operates in conjunctions with other policies including Acceptable Use, Bullying and Harassment and Data Protection.

Definition: e-safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles such as Xbox, PlayStation and Wii.

Safeguarding against these risks is not just an ICT responsibility, it is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

Context

To prepare learners for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life.

However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and learners into contact with a wide variety of influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the learning environment.

Current and emerging technologies in college and more importantly, in many cases used outside the college by learners include:

- Internet websites
- Virtual Learning Environments (VLE)
- Instant messaging

- Social networking sites (E.g. Facebook, Instagram, Twitter etc.)

- E-mails
- Blogs
- Podcasting
- Video broadcasting sites (E.g. Youtube, Vimeo)
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smartphones, iPads and Tablets with e-mail and web applications.
- Personal computers, laptops and mobile phones
- Gaming consoles such as Xbox, PlayStation and Wii.

All of these have potential to help raise standards of teaching and learning, but may equally present challenges to both learners and tutors in terms of keeping themselves safe and secure from external influence as highlighted in Prevent. These challenges include:

Content

- Commercial (adverts, spam, sponsorship, personal information)
- Aggressive (violent/hateful content)
- Sexual (pornographic or unwelcome sexual content)
- Values (bias, racism, misleading info or advice)

Contact

- Commercial (tracking, harvesting personal information)
- Aggressive (being bullied, harassed or stalked, cyber-bullying)
- Sexual (meeting strangers, being groomed)
- Values (self-harm, unwelcome persuasions)

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)
- Aggressive (bullying or harassing another)
- Sexual (creating and uploading inappropriate material)
- Values (providing misleading info or advice)

Others

- Exposure to inappropriate material
- Identity theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising online gambling and financial scams
- Safeguarding issues such as grooming (Children or vulnerable adults)
- Other illegal activities.

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism that would be considered ***inappropriate and restricted*** elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as ***'grooming'*** and may take place over a period of months using chat rooms, social networking sites and mobile phones.

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

1. Roles and Responsibilities

Staff

All teaching and non-teaching staff (including volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour throughout the Academy and following safety procedures.

All Academy staff should:

- Participate in any mandatory e-safety training and awareness raising sessions read, understand, accept and act in accordance with the E-Safety Policy report any suspicion of misuse to the designated persons or line manager
- Refrain from making negative comments about learners or the Academy on any blogs or social networking sites. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of the Academy and/or lowers morale
- Help educate learners in keeping safe, acting as a good role model in their own use of ICT and directing to sites which are appropriate for the use of learning
- Be vigilant in monitoring the content of websites in case there is any unsuitable material
- Be aware of the potential for cyber-bullying in their sessions where malicious messages e.g. through the use of forums on the VLE and social networking sites, or via internal class emails or text messages on mobile phones etc, which can cause hurt or distress.

Learners

Learners are encouraged to access various technologies in sessions, private study and in the completion of assignments and independent research, and are therefore expected to follow the Academy's Acceptable Use Policy. They should participate fully in e-safety activities and report any suspected misuse to a member of staff.

Learners & Staff are expected to:

- Behave in a safe and responsible manner
- Treat equipment with respect
- Use USB/flash memory key(s) only for college purposes
- Be polite and not use e-mail, social media or blogs etc. to make negative comments, bully or insult others

- Use the resources only for educational purposes.

Learners & Staff are expected not to:

- Waste resources including Internet and printers
- Eat or drink when using ICT resources
- Use someone else's login details or share your own
- Have any inappropriate files (e.g. copyrighted or indecent material)
- Attempt to circumvent or "hack" any systems
- Use inappropriate or unacceptable language
- Reveal their personal details or passwords
- Visit websites that are offensive in any way
- Use chat rooms or newsgroups, apart from educational use.
- Do anything that could damage the reputation of the college
- Download anything inappropriate or install any programs.

Breaching these Rules may lead to:

- Withdrawal from the Academy ICT facilities
- Temporary or permanent prevention of access to the relevant pages on the Internet
- Limited or disabled rights where systems are relevant
- Appropriate disciplinary action
- Users should note that breaches of the provisions set out in these Rules may lead to criminal or civil prosecution.

Making an Alert

Once you suspect or know of any e-safety issues, you should normally inform your line manager who will help you to contact a Designated Safeguarding Officer or someone else in authority*, immediately.

In the event of immediate danger this would be the police (999).

Adam Russell **Head of Quality, Learning & Development** **020 7405 0197 ext 383**	**Lili Capelle** **Head of Apprenticeships** **020 7405 0197**
Sarah Arnold **Lead IQA & Tutor** **0121 655 0105**	

If a Designated Safeguarding Officer is not available you should contact the Director or your line manager.

2. ***Designated Safeguarding Officers- E-Safety Leads***

The Designated Safeguarding Officers will lead on E-Safety, where their main roles and responsibilities will include:

- Maintaining the Acceptable Use Policies

- Ensuring that the organisation's policies and procedures include aspects of e-safety.
- Working with the filter system provider to ensure that the filtering is set at the correct level for staff, children, young people and vulnerable adults
- Report issues to the head of the organisation
- Ensure that staff participate in e-safety training
- Ensure that e-safety is included in staff induction
- Monitor and evaluate incidents that occur to inform future safeguarding developments

3. Managing Incidents

The E-Safety leads will ensure that an adult follows these procedures in the event of any misuse of the internet:

Has there been inappropriate contact?

1. Report to the organisation e-safety leads
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3. Contact the parent(s)/carer(s) (If under 18)
4. Contact the police
5. Log the incident
6. Identify support for the child, young person or vulnerable adult

Has someone been bullied?

1. Report to the organisation e-safety leads
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Has someone made malicious/threatening comments? (child/ young person/ vulnerable adult or organisation staff/volunteer)

1. Report to the organisation e-safety leads
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Has an inappropriate/illegal website been viewed?

1. Report to the organisation e-safety leads
2. If illegal, do not log off the computer but disconnect from the electricity supply and contact the police
3. Record the website address as well as the date and time of access
4. If inappropriate, refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s) if they are under 18.
7. Contact the filtering software provider to notify them of the website
8. Log the incident
9. Identify support for the child, young person or vulnerable adult

Has an allegation been made against a member organisation staff/volunteer?

1. Report to the organisation e-safety leads
2. Secure and preserve any evidence
3. Inform the police as appropriate
4. Log the incident
5. Identify support for the child, young person or vulnerable adult

6. ***Relevant legislation:***

- Education Act 1996
- Education Act 2002 (Every Child Matters)
- The Children Act 2004
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990