E-Safety and Acceptable Use of ICT Policy

Last updated: 02/08/2018 / 08/01/2019
Next review: August 2019
By: Paul Stephens

1. Context

WE Bridge Academy is a professional English language school located in Cardiff city centre and accepts students aged from 16+ throughout the year from a variety of different countries.

WE Bridge Academy recognises that the use of internet technologies and communication devices are now seen as a vital life skill and that the use of these can help to enhance communication and the sharing of information. However, WE Bridge Academy is also aware that the use of these technologies have the potential to challenge the definitions and boundaries of learning and teaching.

Current internet technologies and electronic communication devices used by students and staff inside of WE Bridge Academy may include, and is not limited to:

- Internet websites
- Virtual Learning Environments (VLE)
- Instant Messaging (IM)
- Social networking sites (such as Facebook, Instagram, Snapchat and Twitter)
- Email
- Video broadcasting sites (such as YouTube)
- Smart phones with email and web applications
- Tablets and mobile phones with digital cameras
- Laptops and desktop PC's

WE Bridge Academy recognises that all of these have the potential to help improve standards of learning and teaching, but may equally present challenges to both students and staff in terms of keeping safe. The challenges include:

- Exposure to inappropriate or illegal material
- Cyberbullying via websites, social media or mobile phones
- Identity theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising or financial scams (*phishing*)
- Safeguarding issues, such as grooming of under 18s or vulnerable adults
- Other illegal activities

2. Key terminology

Acceptable Use Policy (AUP)
An AUP is a document that outlines a set of rules to be followed by all users of a set of computing resources, which could be a computer network, website or computer system. An AUP clearly states what the user is and is now allowed to do with these resources.

Child Protection
This is part of safeguarding and promoting welfare. This refers to the activity that is undertaken to protect specific children who are suffering, or likely to suffer significant harm.

Children and under 18s
The Children Act 1989 states the legal definition of a 'child' as a 'person under the age of 18. The terms 'child' and 'under 18' are used interchangeably in this policy.

Cyberbullying
This refers to bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers and tablets, as well as communication tools including social media sites, text messages, chat and websites.

Examples of cyberbullying include mean text messages or emails, rumours sent by texts, email or social networking sites, embarrassing pictures or videos posted on websites and the creation of fake profiles.

Designated Safeguarding Lead (DSL)
This person takes overall responsibility for safeguarding and leading the team of Designated Safeguarding Staff (DSS).

Designated Safeguarding Staff (DSS)
WE Bridge Academy has a number of DSS to help lead and co-ordinate safeguarding practice for children and vulnerable adults.

Duty of care
This is the legal obligation to safeguard others from harm while they are in your care.

Digital media
Digital media is digitized content that can be transmitted over the internet or computer networks. This can include text, audio, video and graphics.

E-safety
The safe and responsible use of internet technology and other electronic communications.

Information and Communications Technology (ICT)
ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on.

Stakeholders
All students, staff, volunteers, visitors and contractors who attend, visit or provide services for WE Bridge Academy.

Safeguarding
Safeguarding and promoting the welfare of children is:

- protecting children from harm
- protecting children from that which is not in their best interests
- preventing the impairment of children's health and safety

Social media
Websites and applications that enable users to create and share content or to participate in social networking.

Social networking
The use of websites and other internet services to communicate with other people and make friends.

Vulnerable adults
A person can be considered to be 'vulnerable' if they are "in need of community care services by reason of mental or other disability, age or illness; and is or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation" (*Lord Chancellor's Department, 1997)*. This definition of adult covers all people over 18 years of age.

3. Policy statement

This E-safety and Acceptable Use of ICT Policy relates to all stakeholders of WE Bridge Academy (including students, staff, volunteers, visitors and contractors) who have access to, and are users of internet technologies and electronic communications both in and out of WE Bridge Academy venues where actions relate to WE Bridge Academy activities, or the use of WE Bridge Academy ICT systems.

WE Bridge Academy seeks to maximise the educational benefit that can be obtained by internet technologies and electronic communication devices, while at the same time minimizing any associated risks.

Safety and wellbeing is the collective and individual responsibility of all its stakeholders.

WE Bridge Academy aims to ensure that regardless of age, gender, race, ethnicity, religion or beliefs, sexual orientation, socio-economic background, all stakeholders have a positive and safe learning, teaching and working experience.

As part of this policy, WE Bridge Academy will:

- Promote and prioritise e-safety for all members.
- Establish an understanding of roles and responsibilities in respect of e-safety and ensure everyone is provided with appropriate learning opportunities to recognise, identify and

respond to any concerns regarding to the use of internet technologies and other electronic communications.
- Ensure that appropriate action is taken in the event of any e-safety concerns and support is provides to the individual(s) who raise or disclose the concern.
- Ensure that confidential, detailed and accurate records of all e-safety concerns are maintained and securely stored.
- Ensure that robust e-safety arrangements and AUPs are in operation.
- This policy is available to all stakeholders of WE Bridge Academy.

Failure to comply with this policy and procedures will be addressed immediately and may ultimately result in instant dismissal or exclusion from WE Bridge Academy.

4. Associated policies

This policy operates in conjunction with WE Bridge Academy's Safeguarding Policy, Social Media Policy and Emergency Procedure (cyberattack).

5. Policy review

This policy will be reviewed once a year or following any updates in relevant policies or procedures. Feedback is collected bi-annually from all stakeholders. The policy will be reviewed by the DSL, e-safety coordinator and Chief Executive Officer.

6. Roles and responsibilities

Chief Executive Officer (Dave Henson)
The Chief Executive Officer has a duty of care for ensuring the safety and e-safety of all stakeholders though the day-to-day responsibility for e-safety will be delegated to the e-safety coordinator.

The Chief Executive Officer and other members of the management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Chief Executive Officer is responsible for ensuring that the e-safety coordinators and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues.

The Chief Executive Officer will ensure that there is a system in place to allow for monitoring and support of those who carry out the e-safety monitoring role.

E-safety Coordinator (Paul Stephens)
The role of the e-safety coordinator includes:

- Leading e-safety training and awareness-raising sessions.
- Having day-to-day responsibility for e-safety issues as well as reviewing the school e-safety policies.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

- Making sure that they have an up-to-date awareness of e-safety matters and of current e-safety policy and practices

Staff

All teaching and non-teaching staff (volunteers, suppliers, contractors, interns and temporary staff) are responsible for supporting safe behaviour and e-safety procedures.

All staff should be familiar with the E-safety and Acceptable Use Agreement (AUP) as well as their relevance to WE Bridge Academy's code of conduct and safeguarding policies.

As well as the above, all staff should do the following:

- Participate in any e-safety training and awareness-raising sessions.
- Ensure they have read, understood and signed the E-safety and Acceptable Use of ICT Policy.
- Act in accordance with the E-safety and Acceptable Use of ICT Policy.
- Report any suspected misuse or problems to Chief Executive Officer or E-safety coordinator.
- Refrain from making negative comments about WE Bridge Academy and its stakeholders via any electronic communications (e.g. social networking sites, messaging apps).
- Ensure that any electronic communications with other stakeholders are on a professional level and adhere to the E-safety and Acceptable Use of ICT Policy.
- Help to educate students in keeping safe, especially under 18's and vulnerable groups.
- Help students to understand and follow the E-safety and acceptable use of ICT policies and procedures.
- Monitor students' use of electronic devices such as mobile phones and tablets in lessons and other relevant activities and implement current policies with regards to these devices.

Students

All students are responsible for using WE Bridge's Academy ICT systems in accordance with this policy.

All students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

All students need to understand the importance of adopting good e-safety practice when using electronic communications outside of WE Bridge Academy, and realise that this policy covers their actions outside the academy if related to their membership of the academy.

7. Code of conduct

This code of conduct:

- Assists stakeholders in working safely and responsibly and monitoring their own standards and practice.
- Sets clear expectations of behavior and codes of practice relevant to e-safety and use of ICT.

- Supports stakeholders by giving a clear message that unlawful or unsafe behavior is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

8. Managing internet access and information systems

To ensure that WE Bridge Academy's information systems remain safe:

- The security of WE Bridge Academy's information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Firewalls and filters will be used at all times.
- Unapproved software will not be allowed in work areas or attached to emails.
- All computer equipment is set to automatic updating and installed antivirus software is updated regularly.
- Server is maintained, monitored and serviced by out IT provider, Pisys.

WE Bridge Academy's equipment and systems must not be used:

- For any form of harassment of individuals including colleagues, clients and other stakeholders.
- To download, access, record and/or store material that could be considered racist, sexist, homophobic or likely to be in contravention of discrimination, bullying or harassment legislation.
- To access adult or pornographic material.
- To upload any inappropriate content (including copyrighted or indecent material).
- To install any programs without the prior permission of a designated member of staff.
- To attempt to circumvent or 'hack' any systems.
- WE Bridge Academy reserves right to view all material (including emails of a personal nature) stored in its computer system.

Email
Students and staff must immediately tell a designated member of staff if they receive an offensive email.

Staff will only use official work-provided email accounts to communicate with other stakeholders (including students, parents, carers and third parties).

Emails must not be used to forward inappropriate messages or content to any individual.

Emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in WE Bridge Academy is allowed.

Filtering
WE Bridge Academy's broadband access will include appropriate filtering. If a student or a member of staff discovers an unsuitable site, the URL will be reported to the e-safety coordinator who will record the incident and escalate the concern as appropriate.

The e-safety coordinator will ensure that regular checks are made to ensure that the filtering methods selected are effective.

Mobile phones and personal devices (including laptops and tablets)
The use of mobile phones and other personal devices by students and staff in school will be decided by WE Bridge Academy.

Mobile phones and personal devices will not be used by students during lessons unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.

Staff and other stakeholders must not use their personal phones or devices to contact any students under 18.

Published content and WE Bridge Academy's website
The contact details on the website should be the school address, email and telephone number. Other stakeholder personal information will not be published.

The Chief Executive Officer will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing images of students aged under 18
Photographs of students aged under 18 will be selected carefully and will not enable individual students to be identified. Material used of students aged under 18 will have received prior parental consent, and a record held on the students' file.

The full names of students who are under 18 will not be used anywhere on the website or social media networks.

Social media and social networking
All students will be advised never to give out personal details of any kind which may identify them and/or location. Examples would include real name, address, mobile number, school attended, IM and email address.

All students and staff will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

All students and staff will be advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Staff are required to not post entries that are publicly accessible, which contain negative references to the company, its staff, business activities, clients or products.

Staff must not conduct themselves in a way that is detrimental to the company.
Staff must take care not to allow their interaction on social networking websites to damage working relationships between members of staff and the company's clients or third parties.

Staff must not 'add' any students aged under 18 to their personal social networks. Concern regarding students' use of social networking, social media, and personal publishing sites (in or out of WE Bridge Academy) will be raised with their parents / carers, particularly when concerning students underage use of sites.

9. Policy decisions

Authorising internet access
All staff will be asked to read and sign the relevant e-safety and acceptable use of ICT policy at their induction.

All visitors to WE Bridge Academy who require internet and/or ICT access will be asked to read and sign the E-safety and Acceptable Use of ICT Policy before they are given access.

Assessing risks
WE Bridge Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never appear on a computer that belongs to WE Bridge Academy. WE Bridge Academy cannot accept liability for the material access or any consequences resulting from internet use.

The e-safety coordinator will regularly audit the use of ICT to establish if the E-safety and Acceptable Use of ICT policy is adequate and that the implementation of the policy is appropriate.

Responding to e-safety concerns and incidents
All WE Bridge Academy stakeholders will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, cyberbullying, downloading of illegal content, etc.). The e-safety coordinator will record all reported incidents and actions taken.

The DSL will be informed of any e-safety incidents involving safeguarding concerns and will be dealt with appropriately.

WE Bridge Academy will inform the parents or carers of under 18s of any incidents or concerns as and when required. Any complaint about staff misuse must be referred to the Chief Executive Officer.

Any sanctions will be issued in accordance with WE Bridge Academy's disciplinary procedures. Sanctions can include: interview and counselling by e-safety coordinator / teacher, informing parents or carers and removal of access to internet for a period of time.

Where there is cause for concern that illegal activity has taken place, the police will be contacted.

Managing cyberbullying
Cyberbullying of any member of WE Bridge Academy will not be tolerated and all incidents of cyberbullying need to be reported to the e-safety coordinator.

Any sanctions will be issued in accordance with WE Bridge Academy's disciplinary procedures.

10. Communication policy

Informing students
Our E-safety and Acceptable Use of ICT Policy is communicated to all students at induction and acknowledge this in a dedicated section of their enrolment form, which they must sign.
.
E-safety rules will be posted in all classrooms.

Safe and responsible use of the internet and technology will be reinforced across the curriculum.

Students will be informed that internet use will be monitored. Particular attention to e-safety awareness will be given to students under 18 and students who are considered to be vulnerable.

Informing staff
All staff (including contractors, visitors and volunteers) will read and sign the E-safety and Acceptable Use of ICT Policy at induction.

Staff will be made aware that internet use will be monitored and can be traced to the individual user.

Up-to-date and appropriate staff training in e-safety and acceptable use of ICT will be provided for all members of staff.

All staff will be made aware that their online conduct in and out of the academy could have an impact on their role and reputation within the academy. Civil, legal or disciplinary action could be taken if they are found to bring the academy into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Photography and Filming
At the very least, verbal consent must be obtained from anyone who may appear in videos and photographs taken by the academy. Students and staff may also be required to read, sign and give permission for their image to be used on the relevant GDPR Permission form, which details that their image may be used on social media, our website and in marketing material. Students wishing to film or take photographs in the classroom must seek verbal permission from the teacher first and are advised this at induction.

WE Bridge Academy must never share images with anyone outside of the business without the written consent of the person(s) contained in the images. Third parties wishing to take photographs within the academy must seek verbal permission from the E-Safety Coordinator, Director of Studies or CEO/COO. It should be made clear WE Bridge Academy is not responsible for images taken by third parties. This information should be communicated to both students and staff and informed clearly of why their image is being captured and how it may be used.

Network Support (Pisys)
Support for our server, leased line and I.T. equipment is managed by Pisys. Any support requests should be raised with support@pisys.net who will then confirm the request by email with a support ticket. All requests should be made via the E-Safety Coordinator (ESO). Pisys will verify all support tickets that are raised by anyone other than the ESO before proceeding to work on support requests to protect our systems in line with this policy.

E-safety and Acceptable Use of ICT Policy for Staff

I have read and understood the E-safety and Acceptable Use of ICT Policy and agree to abide by the policy.

I understand that I have a responsibility for my own and others e-safety, especially in regard to under 18s.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand WE Bridge Academy's most recent E-safety and Acceptable Use of ICT Policy.

I will not intentionally visit internet sites that contain offensive, illegal, hateful or inappropriate materials.

I will report any accidental accessing of inappropriate materials to the e-safety coordinator.

I will not copy information from the internet into my work without acknowledging the source (plagiarism and copyright infringement).

I will not download or upload any materials or images that are inappropriate.

I understand that my use of the internet (including distributing or receiving information, school-related or personal) may be monitored for unusual activity, security and/or network management reasons.

I will not use digital technology to write hurtful comments, bully or make threats.

I agree to take care of the hardware and software at WE Bridge Academy.

Signature: _____

Print name: _____

Date: _____