E-safety, Acceptable Use of ICT and Social Media Policy

WE Bridge Academy
Floor 10 Southgate House
Wood Street
Cardiff
CF10 1EW
UK

Last updated: April 2024
Next review: April 2025
By: Murilo Camargo

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 has 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, TikTok, 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 PCs

WE Bridge Academy recognizes 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

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, tablets and smart watches 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 several 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.

Safeguarding

Safeguarding and promoting the welfare of students is:

- protecting them from harm
- protecting them from that which is not in their best interests
- preventing the impairment of their 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 '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.

Policy statement

This E-safety and Acceptable Use of ICT Policy relates to all staff, volunteers, students, visitors and contractors of WE Bridge Academy 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 maximize 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 are the collective and individual responsibility of everyone.

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

As part of this policy, WE Bridge Academy will:

- Promote and prioritize 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 recognize, 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 everyone at 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.

Policy review

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

Roles and responsibilities Managing Director (MD)

The MD has a duty of care for ensuring the safety and e-safety of everyone, though the day-to-day responsibility for e-safety will be delegated to the e-safety coordinator.

The MD will:

- Ensure members of the management team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- Be 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
- 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
- The role of the e-safety coordinator includes:
- Liaising with the Academy IT Support company, Toolk-IT, 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 the MD or E-safety coordinator
- Refrain from making negative comments about WE Bridge Academy via any electronic communications (e.g., social networking sites, messaging apps)
- Ensure that all electronic communications 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 18s 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.

Code of conduct

This code of conduct:

- Assists everyone in working safely and responsibly and monitoring their own standards and practice
- Sets clear expectations of behaviour and codes of practice relevant to e-safety and use of ICT
- Supports everyone by giving a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken

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
- Firewalls and filters will be always used
- 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

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

- For any form of harassment of individuals including staff, students, and visitors
- 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 materials stored in its computer systems

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 relevant to the purpose of their role. 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 must not use their personal phones or devices to contact any students under 18 for non work- related purposes.

Published content and WE Bridge Academy's website

The contact details on the website should be the school address, email, and telephone number.

The MD 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 current students 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, particularly when concerning students underage use of sites

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.

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

- Everyone 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 MD
- 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.

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 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 vulnerable.

Informing staff

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 business. 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 MD. 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 (Toolk-IT)

Support for our server, leased line and I.T. equipment is managed by Toolk-it. Any support requests should be raised with support@toolk-it.net who will then confirm the request by email with a support ticket. All requests should be made via the E-Safety Coordinator (ESO). Toolk-it 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 regarding 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: _____

Social Media

Introduction

Employees of WE Bridge Academy can access social media services and social networking sites at work either through company IT systems or via their own personal equipment.

This social media policy describes the rules governing use of social media at WE Bridge Academy and sets out how staff must behave when using the company's social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff may say about the company on their personal accounts.

This policy should be read alongside other key policies (Emergency Procedure and the Safeguarding Policy). The E-safety and Acceptable ICT Use Policy is particularly relevant to staff using social media.

Why this policy exists

Social media can bring significant benefits to WE Bridge Academy, particularly for building relationships with current and potential customers.

However, it's important that employees who use social media within the company do so in a way that enhances the company's prospects. A misjudged status update can generate complaints, could offend, or damage our reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively.

Policy scope

This policy applies to all staff, contractors, interns, and volunteers at WE Bridge Academy who use social media while working – no matter whether for business or personal reasons. It applies no matter if social media use takes place on company premises, while travelling for business or working from home.

Social media sites and services include, but are not limited to:

- Popular social networks like Twitter and Facebook
- Online review websites like Reevoo and Trustpilot
- Sharing and discussion sites like Delicious and Reddit
- Photographic social networks like Instagram and Snapchat
- Question and answer social networks like Yahoo Answers
- Professional social networks like LinkedIn

Responsibilities

Everyone who operates or is linked to a company social media account or who uses their personal social media accounts at work has a responsibility for implementing this policy. However, the following have key responsibilities:

- The e-safety coordinator is ultimately responsible for ensuring that WE Bridge Academy uses social media safely, appropriately and in line with the company's objectives
- The e-safety coordinator is responsible for monitoring WE Bridge Academy's posts, interactions, and performance and to remove inappropriate content that may appear on our social media sites. Profanity filters are set on the current sites we use including Facebook, Twitter, and Instagram
- The Marketing team are responsible for working with the social media coordinator to communicate marketing ideas and campaigns through our social media channels

General social media guidelines

The power of social media

WE Bridge Academy recognises that social media offers a platform for the company to perform marketing, stay connected with customers, interact, and build a profile online.

WE Bridge Academy encourages employees to use social media to support the company's goals and objectives and represent us in a positive way.

Basic advice

Regardless of which social networks employees are using, or whether they're using business or personal accounts in company time, following these simple rules helps avoid the most common pitfalls:

- Know the social network. Employees should spend time becoming familiar with a social network before contributing. It's important to read any FAQs and understand what is and is not acceptable before posting messages and updates
- If unsure, don't post it. If an employee feels a post or update may cause offence, upset or a compliant – or be otherwise unsuitable – they should not post it. Staff members can always consult the social media coordinator for advice
- Be thoughtful and polite. Observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email
- Look out for security threats. Staff should be on guard for social engineering and phishing attempts. Social networks can also be used to distribute spam and malware. Further details below
- Keep personal use reasonable. Although WE Bridge Academy believes that having employees who are active on social media can be valuable, unless specific to your job role, personal use on social media should be restricted to break times and out of core hours
- Don't make promises without checking. WE Bridge Academy's social media channels are all public, which means anyone can view the content. Employees should not make any promises or commitments on behalf of WE Bridge Academy without checking these promises can be delivered. Direct any enquiries to the social media coordinator
- Handle complex queries via other channels. Social networks are not a good place to resolve complicated enquiries and issues. Once someone makes contact, employees should manage further communication internally (by email, phone or in person)
- Don't escalate things. It's easy to post a quick response to a contentious status update and then regret it. Employees should always take time to think before responding and hold back if there is any doubt at all

Use of WE Bridge Academy's social media accounts

This part of the social media policy covers all use of social media accounts owned and run by the company.

Authorised users

- Only people who have been authorised to use WE Bridge Academy's social networking accounts may do so
- Authorisation to use our social media networking accounts will typically be granted when social media-related tasks form a core part of an employee's job
- Allowing only designated people to use the accounts ensures the company's social media presence is consistent and cohesive

Creating social media accounts

New social media accounts may only be created by the social media coordinator. The company operates its social media presence in line with a strategy that focusses on the most appropriate network, given available resources.

If there is a case to be made for opening a new account, employees should raise this with the social media coordinator.

Purpose of company social media accounts

WE Bridge Academy's social media accounts may be used for many different purposes. In general, employees should only post updates, messages, or otherwise use these accounts when that use is clearly in line with our overall objectives. For instance, employees may use company social media accounts to:

- Respond to customer enquiries and requests for information
- Share relevant articles and other content created by WE Bridge Academy
- Share insightful articles, videos, media, and other content relevant to the business, created by WE Bridge Academy and others
- Provide followers with an insight into what goes on at WE Bridge Academy
- Promote marketing campaigns and, on occasions, special offers
- Support new initiatives

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it and to put those ideas to the social media coordinator.

Inappropriate content and uses

WE Bridge Academy's social media accounts must not be used to share or spread inappropriate content or to take part in activities that could bring the company into disrepute.

WE Bridge Academy should not be seen to favour specific companies, organisations, or individuals. All content should be reviewed before posting.

Use of personal social media accounts at work

The value of social media

WE Bridge Academy recognises that employees' personal social media accounts can generate many benefits. For instance:

- Staff members can make industry contacts that may be useful in their jobs
- Employees can discover content to help them learn and develop in their role
- By posting about the company, staff members can help to increase our presence online

Personal social media rules Acceptable use:

- Employees may use their personal social media accounts for work-related purposes at break times and out of the company's core working hours
- Only staff authorised to use WE Bridge Academy's social media accounts may do so during working hours providing there is a genuine reason to do so (such as posting updates and monitoring interaction)
- Social media should not affect the ability of employees to perform their regular duties

Talking about the company:

- Employees should ensure their social media account does not represent WE Bridge Academy's views or opinions
- Staff may wish to include a disclaimer if posting about WE Bridge Academy: 'the views expressed are my own and do not reflect the views of my employer'

Safe, responsible social media use

The rules in this section apply to:

- Any employees using company social media accounts
- Employees using personal social media accounts during company time

Users must not:

- Create or transmit material that might be defamatory or incur liability for the company
- Post messages, status updates or links to material or content that is inappropriate. Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling, and illegal drugs

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on race, age, sex, religious or political beliefs, origin, disability, sexual orientation, or any other characteristic protected by law.

- Use social media for any illegal or criminal activities
- Send offensive or harassing material to others via social media
- Broadcast unsolicited views on social, political, religious, or other non-business-related matters
- Send or post messages or material that could damage WE Bridge Academy's image or reputatio
- Interact with WE Bridge Academy's competitors in any ways which could be interpreted as being offensive, disrespectful, or rude. Communication with direct competitors should be kept to a minimum
- Discuss colleagues, competitors, customers, or suppliers without their approval
- Post, upload, forward or link to spam, junk email or chain emails and messages
- Users must:
- Gain verbal permission from students aged over 18 before posting their images online
- Check the Parental Permission form for any student aged under 18 to ensure they have consent to appear on social media/marketing material before using their images online

Security and data protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

Maintain confidentiality

Users must not:

- Share or link to any content or information owned by the company that could be considered confidential or commercially sensitive. This might include details of key contacts/agents or information about our future strategy or marketing campaigns
- Share or link to any content or information owned by another company or person that could be considered confidential or commercially sensitive. For example, if a competitor's marketing strategy was leaked online, employees of WE Bridge Academy should not mention it online
- Share or link to data in a way that could breach the company's data protection policy

Protect social accounts

- Company social media accounts must be protected using strong passwords that are changed regularly and only shared with authorised users, if applicable
- Whenever possible, employees should use two-factor authentication (often called phone verification) to safeguard company accounts

Avoid social scams

- Staff should watch for phishing attempts where scammers may attempt to use deception to obtain information relating to either the company or its customers
- Employees should never reveal sensitive details through social media channels. Customer and student identities should always be verified before information is shared or discussed
- Employees should avoid clicking links in posts, updates and direct messages that look suspicious. Users should look out for URLs contained in generic or vague-sounding direct messages

Policy enforcement

WE Bridge Academy reserves the right to monitor how social networks are used and accessed. Additionally, all data relating to social networks written, sent, or received through the company's computer systems and network is part of official company records.

WE Bridge Academy can be legally compelled to show that information to law enforcement agencies or other parties. Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors, and other users may also be held personally liable for violating this policy.