

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

Policy Version	Author	Review Date
Version 1 - March 2011	NH	Annual
Version 2 – May 2017	NH	August 2017
Version 3 - Sept 2019	NH	Sept 2020
Updated April 2020 - April 2021 Reviewed April 2021 – no amendments – Review April 2022		
Version 4 – January 2024	NH	January 2025

Introduction

This policy reflects the safeguarding needs of staff and students at Bridge Training, and works with, and aligns with other key safeguarding and organisational policies, procedures, and standards.

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. Currently the internet technologies young people are using both inside and outside of the classroom include:

- Websites
- Moodle
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- 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 Bridge Training Ltd we understand the responsibility to educate our students on Online Safety and on-line issues; teaching them the appropriate behaviours and skills to enable them to remain both safe and legal when using internet and related technologies, in and beyond the context of the classroom.

Everybody at Bridge Training 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 staff, visitors and

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

students) are inclusive of both fixed and mobile internet; technologies provided by Bridge Training (such as PCs, laptops, whiteboards, digital video equipment, etc); and technologies owned by students and staff but brought onto the Bridge Training premises (such as laptops, mobile phones, portable media players, etc). The requirement to ensure that young people can use technologies appropriately and safely, should be addressed as part of the wider duty of care. This policy should ensure safe and appropriate use.

At Bridge Training we hold data on students and staff 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 Bridge Training. This can make it more difficult to use technology to benefit students.

The implementation of this strategy involves all stakeholders in Bridge Training Ltd involved in education and/or activities.

Purpose

The purpose of this policy is to provide safety regulations for staff and students who use Bridge Training Ltd and the work we do with students and families as part of its activities to:

- Ensure the safety and wellbeing of our staff and students is paramount when using the internet, social media, or mobile devices.
- provide staff, volunteers and visitors with the overarching principles that guide our approach to online safety.
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The use of these new technologies can put young people at risk therefore this policy addresses some of the dangers they may face, including:

- Access to illegal, harmful, or inappropriate images
- Unauthorised access to, or loss of, or inappropriate sharing of personal information
- Access to harmful websites, for example those devoted to weapons production, how to take one's own life or promoting high risk behaviours.
- The risk of being subject to grooming via the internet, and possibly meeting high risk individuals offline
- The sharing and/or distribution of personal images without the individuals consent or knowledge.
- Inappropriate communication with others (including strangers).
- Cyber bullying
- Access to unsuitable video/internet games
- Inability to evaluate the accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- Illegal downloading of files
- The potential for excessive/obsessive use

The aim of the Online Safety policy should be to build a student's resilience to risk through good educational provision. Bridge Training must provide the necessary safeguards to help ensure that everything that could reasonably be expected of the organisation has been done to manage and reduce risk.

Legal framework

This policy has been drawn up based on legislation, policy and guidance that seeks to protect students in England. Summaries of the key legislation and guidance are available on:

- online abuse
- bullying
- Student protection.

We believe that:

- Our students should never experience abuse of any kind.
- Our students should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges.
- we have a duty to ensure that all staff and students involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep staff and students safe online, whether they are using Bridge Training's network and/or devices.
- working in partnership with our students, staff, their parents, carers, and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- Our students, regardless of age, disability, gender, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.

Keeping students and staff safe

We will seek to keep students and young people safe by:

- providing clear and specific directions to staff, students, and volunteers on how to behave online through our behaviour code.
- supporting and encouraging students using the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- supporting and encouraging parents and carers to do what they can to keep their students safe online.

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- developing an online safety agreement for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour.
- reviewing and updating the security of our information systems regularly
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff, Student, and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse, and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders, and our organisation into account.
- reviewing the plan developed to address online abuse at regular intervals, to ensure that any problems have been resolved in the long term.

This Online Safety policy should be used in conjunction with all other student protection and Safeguarding policies.

Monitoring

All internet activity is logged by Bridge Training and our Internet Provider. Web pages can be traced for up to four days after being viewed, and emails for up to 18 months. Classroom Cloud is installed on teacher's computers to monitor students screens to ensure that they are on task.

A breach or suspected breach of policy by a Bridge Training employee, contractor or student may result in the temporary or permanent withdrawal of ICT hardware, software, or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with Bridge Training's Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Any teacher who suspects a student is accessing inappropriate material can request an activity report, if there is cause for concern, this is dealt with in accordance with the standard behaviour procedures. Serious incidents are dealt with by the Designated Safeguarding Lead and/or Head of Curriculum. Sanctions will be used according to the severity of the offence.

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 Head of Safeguarding or a member of the Senior Leadership Team and the IT Technical

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

Support Manager

Additionally, all security breaches, lost/stolen equipment, or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head of Finance and Quality and the IT Technical Support Manager.

Computer Viruses

All files downloaded from the Internet, received via e-mail (from an unknown source) or on removable media (e.g. USB memory sticks etc) must be checked for any viruses using Bridge Training provided anti-virus software before using them. Staff should never interfere with any anti-virus software installed on the ICT equipment.

If your machine is not routinely connected to the Bridge Training network, you must make provision for regular virus updates.

If you suspect there may be a virus on any of Bridge Trainings ICT equipment, stop using the equipment and contact IT Technical Support Manager immediately. The IT Technical Support Manager will advise you of what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of data stored on Bridge Training systems is something that the organisation takes very seriously. Therefore

- Bridge Training gives relevant staff access to its Management Information System (and other associated Software) eg Pro-Suite, CPOMS, BKSB etc with a unique ID and password and it is the responsibility of everyone to keep passwords safe and secure.
- Bridge Training gives relevant access to secure folders on the T Drive and Bridge Training Server
- Staff are aware of their responsibility when accessing personal/sensitive data.
- Staff should keep all Bridge Training students' and staff data secure. This includes all personal, sensitive, confidential, or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive and confidential information contained in documents copied, scanned or printed.
- Anyone expecting a confidential/sensitive email should use an encrypted email tool.

Disposal of ICT Equipment

All redundant ICT equipment that may have held personal data will have the

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

storage media over written multiple times and the hard drive drilled to ensure the data is irretrievably destroyed. Therefore:

- Disposal of any ICT equipment will conform to:
 - The Waste Electrical and Electronic Equipment Regulations 2006
 - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
 - General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
 - Electricity at Work Regulations 1989
- Bridge Training will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- Bridge Training's disposal record will include:
 - Date item disposed of
 - Authorisation for disposal, including:
 - verification of software licensing / serial number
 - personal data likely to be held on the storage media? ¹
 - How it was disposed of eg waste, gift, sale
 - Name of person &/or organisation who received disposed item.
- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Email

Bridge Training gives all staff and students their own e-mail account to use for all Bridge Training business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoid 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 (staff and students) and recipients, all mail is filtered; if necessary, e-mail histories can be traced. The Bridge Training email account should be the account that is used for all Bridge Training business, you **MUST NOT** use a private email address for the use of any Bridge Training business.

- Under no circumstances should staff contact students, parents or conduct any Bridge Training related business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on headed paper would.
- Any students using e-mail are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication or arrange to meet anyone without specific

¹ if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

permission. A student must immediately tell a member of Bridge Training staff if they receive an offensive e-mail.

- Staff must inform a member of the SLT if they receive an offensive e-mail.
- However, if you access your work e-mail (whether directly, through webmail when away from the office or on non-Bridge Training hardware) Bridge Training's e-mail policy still applies.

Students are provided with individual Bridge Training email addresses for educational use and must immediately report, to a teacher if they receive any email that makes them feel uncomfortable, is suspicious, offensive, threatening or bullying in nature and must not respond to any such email.

Any communication between staff and students or parents / carers (email, Pro-Suite etc) must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not, under any circumstances, be used for these communications.

Sending Emails

- Use your own Bridge Training e-mail account so that you are clearly identified as the originator of a message.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mails.
- Bridge Training e-mail is not to be used for personal advertising or for personal use or on behalf of anyone else.

Receiving Emails

- Check your e-mail regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult the IT Technical Support Manager first.
- Do not use e-mail systems to store attachments. Detach and save business related work to the appropriate folder.

Emailing Personal, Sensitive or Confidential Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not permitted and should be avoided where possible.
- The use of Hotmail, BT Internet, or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.
- Where your conclusion is that e-mail must be used to transmit such data, exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Do not copy or forward the e-mail to any more recipients than is necessary.
- Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail or encrypted email.
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt

Equal Opportunities

Bridge Training endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of Bridge Training's Online Safety rules. However, staff are aware that students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues, this will be done through PSHE.

Online Safety Roles & Responsibilities

As Online Safety is an important aspect of strategic leadership within Bridge Training, the Senior Leadership Team have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety co-ordinator is the Head of Safeguarding. All members of Bridge Training have been made aware of who holds this post. It is the role of the Online Safety co-ordinator to keep abreast of current issues and guidance.

This policy, supported by the Bridge Training's acceptable use agreements for staff, visitors and students, is to protect the interests and safety of Bridge Training.

Online Safety in Practice

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to students on a regular and meaningful basis. Therefore

- Online Safety is embedded within our curriculum, and we continually look for new opportunities to promote Online Safety.
- Bridge Training provides opportunities within a range of curriculum areas to teach about Online Safety
- Educating students on the dangers of technologies that maybe encountered outside of Bridge Training is done informally when opportunities arise and as part of the curriculum via PSHE.
- Students are aware of the relevant legislation at induction when using the internet such as data protection which may limit what they want to do but also serves to protect them.

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling 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 abuse. They 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, tutor, or an organisation such as Studentline or using the CEOP report abuse button.
- Information for Online is available on our website www.bridgetrainingltd.co.uk on the Parent Page.

Online Safety CPD for BTL Staff

New staff receive information on the organisation's acceptable use policy as part of their induction and all staff have been made aware of individual responsibilities relating to the safeguarding of students within the context of Online Safety and know what to do in the event of misuse of technology by any member of Bridge Training. All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

Managing Online Safety

We aim to

- embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.
- Introduce the policy to students during Induction and periodically throughout their training at Bridge Training
- Online Safety posters will be prominently displayed.

There will be no tolerance of cyber-bullying. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential to report it to the Head of safeguarding as soon as possible and it will be dealt with through normal behaviour / disciplinary procedures.

Incident Reporting

Any security breaches or attempts, loss of equipment, unauthorised use or suspected misuse of ICT, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be immediately reported to a member of the Senior Leadership Team and .

Complaints

Complaints and/or issues relating to Online Safety should be made to the Online Safety co-ordinator or your Line Manager. All incidents should be logged and stored in a confidential file.

Inappropriate Material

- All users (staff and students) are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head of Safeguarding.

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head of Safeguarding and escalated to the relevant Senior Manager, depending on the seriousness of the offence; investigation by the Senior Leadership Team, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users (staff and students) are made aware of sanctions relating to the misuse or misconduct through their Induction.

Internet Access

The internet is an open communication medium, available to all, always. 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.

Internet Use

BTL enables students to have supervised access to Internet resources (where reasonable) through the organisation's fixed internet technology (staff may preview any recommended sites before use). Raw image searches are discouraged when working with students.

If Internet based activities are set for home study

- All users (staff and students) must always observe software copyright. It is illegal to copy or distribute Bridge Training software or illegal software from other sources.
- All users (staff and students) must observe copyright of materials from electronic resources.
- 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.
- Online gambling or gaming is not allowed on any Bridge Training equipment.

Infrastructure

Bridge Training also employs some additional web filtering which is the responsibility of the IT Technical Support Manager. It is also aware of its responsibility when monitoring staff communication under current legislation and considers relevant legislation:

- Staff and students are aware that Bridge Training based email and internet activity can be monitored and explored further if required.
- Bridge Training does not allow students access to internet logs.
- Bridge Training uses management control tools (Classroom Cloud) for controlling and monitoring workstations.

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- If staff and/or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to Head of Safeguarding or teacher as appropriate.
- It is the responsibility of Bridge Training Ltd, to ensure that Anti-virus protection is installed and kept up to date on equipment.

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 Bridge Training's responsibility 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 IT Technical Support Manager for a safety check first.

Students and staff are not permitted to download programs or files on Bridge Trainings based technologies without seeking prior permission from their teacher.

If there are any issues related to viruses or anti-virus software, the IT Technical Support Manager should be informed.

Managing Social Networking Sites

Social networking sites, 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 (staff and students), including themselves, from these sites:

- At present, Bridge Training endeavors to deny access to social networking sites to students when within Bridge Training.
- All students are advised to be cautious about the information given by others on sites, for example users (staff and students) not being who they say they are.
- Students are taught to avoid placing images of themselves and/or staff (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), details about Bridge Training's location, 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 and staff are asked to report any incidents of bullying to Bridge Training/parents/carers/police.
- Staff may only communicate with students on social networking sites via

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

the controlled group site that students can join. No member of staff is permitted to 'add' a student as a friend, or attempt to send, or reply to, a personal message from/to a student unless it is through the group page.

- Any concerns that a member of staff may have about a student, should be reported to the Head of Safeguarding, to investigate further if we believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of Bridge Training and also aware of their responsibilities:
- Parents/carers of students aged between 14-16 are required to decide as to whether they consent to images of their student being taken/used in the public domain (e.g., on Bridge Training's website/marketing literature)
- BTL disseminates information to parents relating to Online Safety where appropriate in the form of;
 - Information and celebration evenings/Open Days
 - Posters
 - Website postings / Parents Page

Passwords

- Always use your own personal passwords to access computer-based services.
- Make sure you enter your personal passwords each time you log on. 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 the authorised IT Technical Support Manager 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 contain a mixture of six characters/numbers/symbols and be difficult to guess.

If you think your password may have been compromised or someone else has become aware of your password this MUST be reported to the IT Technical Support Manager

Password Security

Password security is essential for staff and students, particularly as they can access and use data. Staff and students are expected to have secure passwords which are not shared with anyone.

- All users (staff and students) read and sign an Acceptable Use Agreement to demonstrate that they have understood the Online Safety Policy.
- Users are provided with an individual email, and Management Information System (eg. Pro-Suite - where appropriate) log-in username. They are also

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

expected to use a personal password and keep it private.

- Students are not allowed to deliberately access on-line materials or files on the Bridge Training network of their peers, tutors or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of information contained on the Bridge Training network and the MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users (staff and students) must also make sure that workstations are not left unattended and are locked.

Personal or Sensitive Information - Protecting Personal, Confidential, Sensitive or Classified Information

Members of staff may need to access confidential information about a student through either the MIS or email. It is vital that this information is always kept confidential and secure. This can be done in the following ways:

- Ensure that any Bridge Training 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 and confidential information you disclose or share with others.
- Ensure that personal, sensitive and confidential information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, and confidential information contained in documents you fax, copy, scan, or print. This is particularly important when shared copiers are used and when access is from a non-Bridge Training environment.
- Only download personal data from systems if expressly authorised to do so.
- You must not post on the internet personal, sensitive and confidential, 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, and confidential information.
- Ensure hard copies of data are securely stored in confidential files which can be locked away.

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

- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- 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.
- Only under exceptional circumstances and with permission from a member

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

of the Senior Leadership Team, permission will be granted for staff to work from home and access personal and sensitive data.

Remote Access

Remote access to our IT systems is less secure, therefore making it susceptible to cyber-attacks, including unauthorised access, data breaches and malware infections. It is **YOUR** responsibility to ensure the integrity of our data for all activity via the remote access facility, including sensitivity of data. If data is breached or unauthorised access is granted, then Policy 2.1 GDPR will be enforced. You are responsible for:

- Only use equipment with an appropriate level of security for remote access (Bridge Training equipment)
- To prevent unauthorised access to Bridge Training's data systems, keep all access information such as telephone numbers, logon IDs and passwords confidential and **do not** disclose them to anyone.
- Do not let anyone have access to and/or allow them to logon to Bridge Training laptops and equipment.
- Do not leave your laptop and/or equipment unattended if connected to the remote access facility, if you need to leave your laptop, please ensure that you are logged out of 'remote' and the screen is locked.
- Select passwords 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.
- Always protect Bridge Training information and data, including any printed material produced while using the remote access facility. Take particular care when access is from a non-Bridge Training environment.

Safe Use of Images – Photographic and Video

Students and Staff take and use digital / video images to support educational aims, but must follow Bridge Training policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Bridge Training equipment and NOT personal phones.

Written permission from students /parents or carers will be obtained on an 'opt in' basis before photographs of students is published on the Bridge Training website and/or Social Media platforms or used for publicity that reasonably celebrates success and promotes the work of Bridge Training. Consent is requested on our induction form.

Publishing Student's Images and Work

During Induction, all parents/carers will be asked to give permission to use their work/photos in the following ways:

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

- On the Bridge Training website/Social Media Platforms etc
- In the Bridge Training prospectus and other printed publications that Bridge Training may produce for promotional purposes.
- In display material that may be used in Bridge Training's communal areas
- In display material that may be used in external areas, ie exhibitions promoting Bridge Training
- General media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the student attends Bridge Training unless there is a change in their circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

- Parents/ carers may withdraw permission, in writing, at any time.
- E-mail and postal addresses of students will not be published, nor their full names.
- Before posting student work on the Internet, a check will be made to ensure that permission has been given for work to be displayed.

CCTV

Bridge Training uses CCTV for security and safety. Notification of CCTV use is displayed on the main entrance doors.

Equipment

As a user of ICT, you are responsible for any activity undertaken on the ICT equipment provided to you. ICT equipment issued to staff is logged and serial numbers recorded as part of the inventory. Please ensure:

- That all ICT equipment that you use is kept physically secure
- 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 Bridge Training's network. You are responsible for the backup and restoration of any of your data that is not held on the network.
- Personal or sensitive data should not be stored on local drives.
- It is recommended that a time-locking screensaver is applied to all machines. Any ICT accessing personal data must have a locking screensaver as must any user profiles.
- On termination of employment or resignation, return all ICT equipment to your manager within 24 hours of leaving. 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 and/or students is the responsibility of

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

the appropriate Line Manager and/or teacher to maintain allocation, damage, theft and recovering and returning equipment when no longer needed.

Portable ICT Equipment

This section covers such items as laptops, tablets, phones 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 Bridge Trainings systems and hardware will be monitored in accordance with policy.
- Staff must ensure that all data is stored on the Bridge Training 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, the best practice is to place the laptop in the boot of your car before starting your journey.
- 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 IT Technical Support Manager, fully licensed, and only carried out by the IT Technical Support Manager.
- In areas where there are likely to be members of the public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Personal Mobile Devices (including phones)

- Bridge Training allows staff and students to bring in personal mobile phones and devices for their own use. Under no circumstances does Bridge Training allow a member of staff to contact a student or parent/carer using their personal device
- Students are allowed to bring personal mobile devices/phones into Bridge Training but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- Bridge Training is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate text and/or social media messages between any members of Bridge Training is not allowed.
- Users (staff and students) bringing personal devices into Bridge Training must ensure there is no inappropriate or illegal content on the device.

Addendum

Only in VERY exceptional circumstances eg a Lockdown situation and/or where Bridge Training staff are required to work from home and have no alternative way of contacting students, it is permitted that they can use their personal mobile

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

phones to do so, but must adhere to the following:

- Block their number from appearing on the student's phone by adding 141 before the number dialed.
- Upon returning to work and/or the end of a Lockdown situation, any student numbers stored on the staff member's personal phone must be deleted and work telephones used from there-on-in.

Bridge Training Provided Mobile Devices (including phones)

You are responsible for the security of your work mobile phone. Always set the PIN code on the mobile phone and do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any work mobile phone equipment immediately.
- Work SIM cards must only be used in Bridge Training provided mobile phones.
- You must not send text messages to premium rate services.
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.
- The sending of inappropriate text messages between any members of Bridge Training is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of Bridge Training.
- Where Bridge Training provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used.
- Where Bridge Training provides a laptop and/or a tablet for staff, only this device may be used to conduct work business outside of Bridge Training.

Removable Media

If storing/transferring personal, sensitive, confidential, or classified information using Removable Media:

- Only use recommended removable media
- Store all removable media securely.
- Removable media must be disposed of securely by the IT Technical Support Manager.

Servers

Bridge Training protects its servers by

- Keeping servers in a locked and secure environment
- Limit access rights which is password protected
- Having appropriate security software installed
- Data is backed up regularly.
- Back up media is stored on and off-site in secure locations.

Systems and Access

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

You are responsible for all activity on Bridge Training systems carried out under any access/account rights assigned to you, whether accessed via Bridge Training ICT equipment.

- Do not allow any unauthorised person to use Bridge Training ICT facilities and services that have been provided to you.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from Bridge Training ICT equipment any material that is, or may be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to Bridge Training or may bring Bridge Training into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of Bridge Training's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on Bridge Training systems, hardware or used in relation to Bridge Training business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

Computer History Check

Once a week a maximum of 3 staff members computers will be randomly selected to undergo a surfing history to check for inappropriate material. A weekly log is kept tracking computer and ICT systems checked.

If inappropriate material is uncovered Bridge Training will record dates and times and screen-prints/photos taken. This information will be passed onto the Designated Safeguarding Lead and access to the computer will be restricted until the incident has been fully investigated.

Staff - Telephone Services

- You may make or receive personal telephone calls provided they are infrequent, kept as brief as possible and do not cause annoyance to others.
- Bridge Training telephones are provided specifically for Bridge Training business purposes and personal usage is a privilege that will be withdrawn if abused.
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

qualifies as admissible evidence in slander law cases

Artificial Intelligence

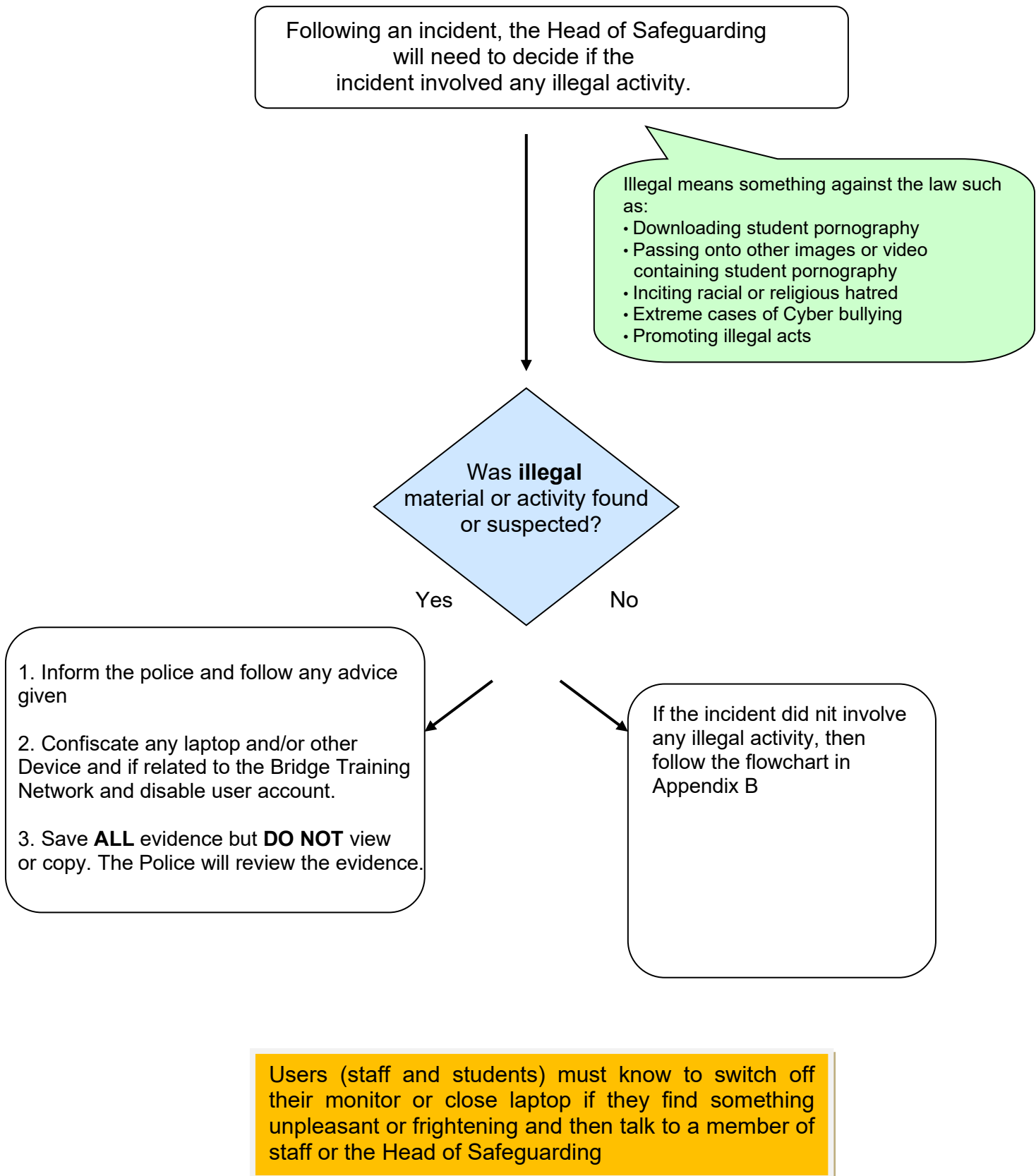
Bridge Training Ltd is committed to harnessing the power of Artificial Intelligence (AI) for the benefit of the student, fostering innovation, and ensuring responsible and ethical use of AI technologies.

We will prioritise the security of our AI systems to prevent unauthorised access, data breaches and malicious use. Regular security checks will be made, and updates conducted to ensure the robustness of AI technology.

Policy: 2.3 – E-Safety / Data Security / On-Line Safety

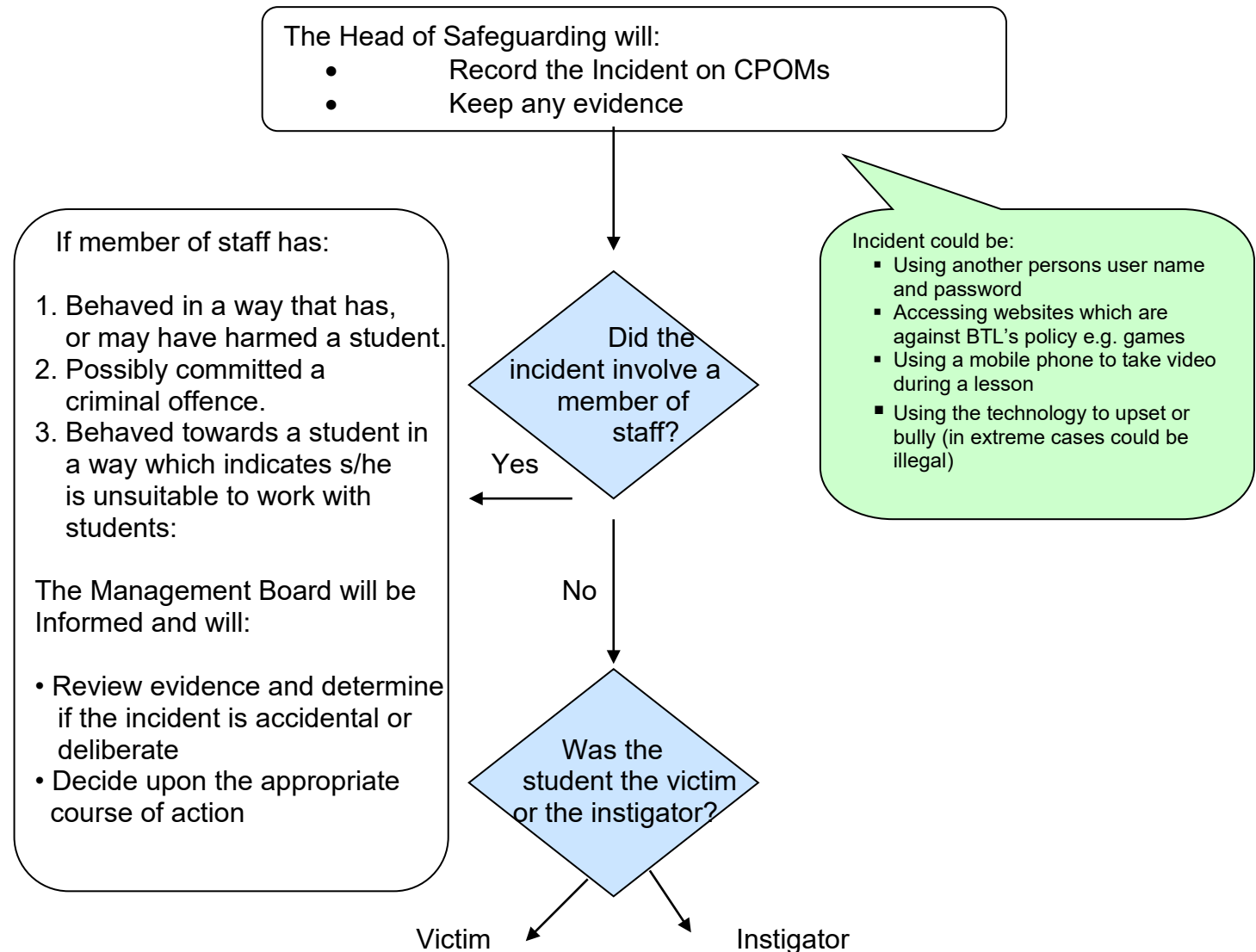
Flowchart A

Bridge Training Flowchart to support decisions related to an Illegal online incident for Teachers, Head of Safeguarding and Senior Managers



Policy: 2.3 – E-Safety / Data Security / On-Line Safety

Flowchart B



In – house action to support student by one or more of the following:
Teacher
ICT Support
Senior Manager or member of the Advisory Board
Safeguarding (A Cambridge / M Harrod)

The device will be confiscated, if appropriate
Parents/ carer informed as appropriate

Review Incident and identify if other learners were involved.
Decide appropriate sanctions and/or support based on Bridge Training guidelines.
Inform parents/carers if serious or persistent incident.
Review procedures/policies to develop best practice

Users (staff and students) must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff