E-Safety Policy

Version	7
Title of Policy	E-Safety
Policy Owner	Emma Grey
Date of Authorisation	31st August 2023
Authorised by	Kerry Bentley
Date for Review	August 2024

Introduction

DBC Training recognises the benefits and opportunities which new technologies offer to programme delivery. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read alongside other relevant DBC policies e.g. Safeguarding, IT Policy, Acceptable Behaviour, Disciplinary and Computer Usage Policy.

Policy Review

A full review will be carried out at least once a year or with any legal or formal guidance updates. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded. These records are stored centrally on the Exec drive and only relevant members of staff have access.

Policy Scope

The policy applies to all learners and staff members of DBC Training who have access to the IT systems, both on the premises and remotely. The policy also includes those who use company IT equipment to access the internet e.g. mobile phone, laptop or iPad. Any user of our IT systems must adhere to and sign a hard copy of the e-Safety Rules and the Acceptable Use Agreement. The e-Safety Policy applies to all use of the internet and the use of all forms of electronic communication such as email, mobile phones, social media sites and Virtual Learning Environment.

Definition of E-Safety

The term e-safety is defined for the purposes of this policy is the process of limiting the risks to all internet users, especially young people and vulnerable adults. Digital and Mobile Technologies (DMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection. It is also to protect the IT system itself e.g. to prevent the downloading and attempt to install unsafe or potentially harmful software.

E-safety risks can be summarised under the following three headings:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films

Contact

- Grooming using communication technologies, potentially leading to sexual assault and/or child prostitution
- Bullying via websites, mobile phones or other forms of communication device

Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Roles and Responsibilities

There are clear lines of responsibility for e-safety within DBC. The first point of contact should be the Designated Safeguarding Lead (DSL). All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All delivery staff are required to include e-safety as part of the induction process and review learner knowledge at reviews. Our DSL sends a weekly Safeguarding update out to all staff which captures the topical issues that have arisen that can be utilised and fed into sessions with learners and shared with employers. Teaching staff are to deliver e-safety sessions to learners and to read through and adhere to the incident reporting procedure as contained in appendix D. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. They are advised at Induction where the policy can be found. In most cases, this will be the DSL. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the DSL may be asked to intervene with appropriate additional support from external agencies.

Designated Safeguarding Lead (DSL):

The DSL is responsible for dealing with any e-safety concerns that are raised either through the automated safeguarding system that monitors student machines and in person, in line with the Safeguarding policy and in the handling of such concerns, will liaise with the local authority and other external agencies using effective and appropriate information sharing.

The automated system will flag any unsafe categorised websites of any device connected to the Wi-Fi regardless if this is an internal or external device.

Staff:

All staff are responsible for using DBC's IT systems and mobile devices in accordance with the IT Policy.

All digital communications with learners must be professional at all times and be carried out in line with the IT Policy. Online communication with learners is restricted and only via official company IT System e.g. Company provided e-mail and Microsoft Teams. External platforms such as social media sites are not to be used to communicate with learners with the exception of Linkedin if the contact is strictly in a professional capacity. Any company social media site will have authorised staff to act as moderators and to respond to learners.

This policy will, however, be monitored and kept under review.

All staff should apply relevant DBC policies and understand the incident reporting procedures. All incidents discovered or staff are made aware of must be reported to the DSL and/or line manager without delay. Further information is available at appendix D.

Security

DBC Training will do all that it can to make sure the IT network is safe and secure. All staff machines currently accredited under Cyber Essentials Plus and are monitored via an external IT company SpudIT. Using both site wide firewall-based traffic filtering, in additional to managed anti-virus currently on staff machines, is used to achieve web filtering, or category-based content filtering, an annual review of security software used to ensure it is fit for purpose. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of company systems and information. Digital communications, including email and internet postings are routinely monitored in line with the IT policy.

Risk Assessment

In making use of new technologies and external online platforms, all staff must first carry out a risk assessment for e-safety as contained in appendix C. This consists of a series of questions for the requester to answer as well as a section in which they can record any relevant comments or evidence. A risk assessment must also be carried out where a learner is learning off site e.g.

work based learning or on work placement. All forms must be submitted to the Skills & Quality Director for consideration and approval.

Behaviour

DBC Training will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the learner and staff disciplinary procedures.

Where conduct is found to be unacceptable, DBC will deal with the matter internally. Where conduct is considered illegal, DBC will report the matter to the police and other relevant statutory bodies e.g. Prevent Officer. The grid at appendix B makes it clear what sanctions will be applied for specific behaviours.

An acceptable usage policy appears at the time of login for student and staff devices to ensure all are aware.

Communications

DBC Training requires all users (including staff) of IT to adhere to appendix A which states clearly when email, mobile phones, social media sites, games consoles, chatrooms, video conferencing and web cameras may be used during the day.

Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and is encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). Staff are responsible to ensure there is no copyright infringements prior to the use of images.

All learners will receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Learner's knowledge will be checked as part of the review process to ensure understanding.

Delivery staff will provide information to learners on the appropriate use of images; this includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

Learner photographs can be copied, downloaded, shared or distributed only with signed parental permission for under 18s and signed permission from learners over 18. This is obtained on during the enrolment process.

Personal Information

Personal information is information about a particular living person. DBC Training collects and stores personal information for contractual and examining board purposes. The information will include names, dates of birth, email addresses, assessed materials and so on. DBC will keep information safe and secure and will share this information only with funding body, examining board or main contractor as required for the purpose. Most funding organisation require data to be kept securely on a database for up to 10 years, of which consent for this is obtained from the learner at the point of enrolment.

Learner images are only used by the company when a signed consent form is obtained by the learner. The individual learner will consent to their image being used for up to 3 years.

No personal information can be posted to the college website/without the signed consent of learner or parent dependent on age of learner.

Only names and work email addresses of (senior) staff will appear on our website.

Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Any personal information of individuals that has to be transported offsite will be password protected if emailed or the use of secure mail service if posted. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period.

All company mobile devices such as a laptop etc are require to be encrypted and password protected.

USB Drives are not to be used within the business.

No learner personal information or company data is to be accessed at any time via a personal mobile device.

When offsite all company data should be accessed via the SharePoint website behind recommended security (2-factor authentication). No company data can be synced locally.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection and IT policy. All data stored within SharePoint and OneDrive is retained via the backup system based on the length required by the funding or examination body.

Monitoring and Filtering

DBC Training has installed a system of monitoring and filtering of all IT systems utilising the DBC network, this includes staff and learners.

Any inappropriate searches are flagged to nominated staff members, a bank of key phrases and words have been registered into the monitoring software and should any of these be entered into any search engine or be used as part of online chats through the network, they will be reported, all devices are named and therefore the individuals can be pinpointed and questioned on their usage and purpose for the search.

Flags as of 1st September 2023 are being formally recorded and comments added to ensure they have all had initial questioning completed. This record will allow us to recognise patterns of behaviour, which can be followed up for repeated incidents.

Those flags that pose a risk or a concern that needs ongoing monitoring or further action will then instigate the Cause for Concern or Safeguarding process.

Learner and staff inductions have been updated to inform all of this process.

Incidents and Response

Where an e-safety incident is reported to DBC this matter will be dealt with very seriously. DBC Training will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or assessor or the Designated Safeguarding Lead. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, DBC will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. The chart in appendix B lists behaviours and their consequences. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Social Media Guidance

Staff and learners should be able to enjoy the benefits of social networking whilst understanding the standards of conduct expected by the Centre.

In terms of IT security, there are controls in place to greatly reduce the potential of a vulnerability. These controls include no user has local administration rights, Anti-virus is installed and also manages any website categorisation to block unsafe sites, and general user training.

General advice

- Staff and learners should apply the same standards of conduct online as they are expected to apply offline.
- Staff should be familiar with privacy settings of social networking platforms and should ensure that these are appropriate for both content and intended audience.
- Social networking platforms are in the public domain and it is not always possible to be sure what is being viewed, shared or archived, even if material is posted on a closed profile or group. There can be no reasonable expectation that posts will remain private and will not be passed on to other people, intentionally or otherwise. Material published online may have the potential to be available publicly, indefinitely.
- Learners and staff are responsible for their words and actions in an online environment and are therefore advised to consider their use of language and phrasing, and whether any comment, photograph or video they are about to post on a social networking site is something they would want fellow learners, colleagues and other employees, their manager or people outside the company to see.
- Inappropriate behaviour via social media may constitute harassment and bullying and can be reported to the Designated Safeguarding Officer.
- DBC Training recognises that members of staff may occasionally wish to use social media for personal use at their place of work, by means of the company's computers, networks and other IT resources and communications systems. Such incidental and occasional use of these systems is permitted, provided that: it is not excessive, does not disrupt, distract or is intrusive to the conduct of business and/or work colleagues (for example, due to volume, frequency or cost), such communications do not bring the company into disrepute. Please refer to the Code of Conduct for more information.
- Staff should not post messages, status updates or links to material or content which is deemed to be inappropriate. Content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism or materials relating to cults, gambling or illegal drugs. Inappropriate content or material also covers any text, images or other media that would reasonably offend someone on the basis of race, age, sex, religion or belief, disability, sexual orientation, gender reassignment, marriage or civil partnership, pregnancy and maternity or any other characteristic protected by law.
- Staff have the right to freedom of thought, opinion and expression and can use social media as a means of communicating these. However, staff should be aware that when posting on social media or forwarding/publishing other's opinions or articles for academic debate (eg re-tweeting) then the same requirements on not posting or linking to inappropriate content still apply.
- Staff or learners should not engage in illegal activity through social media or engage in any activity that promotes terrorism. The very fact of possessing or disseminating terrorist material may be sufficient to warrant an investigation by the police and a member of staff or

learner would be put in the position of having to advance a credible defence. More information can be found in our Safeguarding and Prevent policy.

- When disagreeing with others' opinions, remain appropriate and polite. If you find yourself in a situation online that looks as if it may be becoming antagonistic, do not get overly defensive and do not disengage from the conversation abruptly; ask the Designated Safeguarding Officer or Skills & Quality Director for advice and/or disengage from the dialogue in a polite manner that reflects well on the business.
- If you want to write about competitor institutions, make sure you behave diplomatically, have the facts straight and that you have the appropriate permissions for DBC Training Board.
- Never comment on anything related to legal matters, litigation or any parties the business may be in dispute with.
- Apologise quickly and honestly for any mistakes you make and learn from them for future social media activity.
- If you are concerned that there has been a misuse of social media by another colleague or learner, then you can report this to the Designated Safeguarding Officer or the Skills & Quality Director.
- Be smart about protecting yourself, your privacy, and DBC Training's confidential information. What you publish is widely accessible and will be around for a long time, so consider the content carefully.
- Watch out for phishing attempts, where scammers may attempt to use deception to obtain information relating to you or the business.
- Avoid clicking links in posts, updates and direct messages that look suspicious. In particular, you should look out for URL's contained in generic or vague-sounding direct messages.
- Use a strong password, use different passwords for different applications, never share your password, and log out when you have finished actively using a system. All staff devices currently have 2-factor authentication enabled to increase security.
- Be careful about what you share. Don't reveal sensitive personal information i.e.: home address, financial information, phone number. The more you post the easier it is to have your identity stolen.
- Be selective with friend requests. If you don't know the person, don't accept their request. It could be a fake account.
- Do a search on yourself; you may be surprised. If you feel you have too much information out there, you can always restrict your online profile.

Legislation

The legal framework for the role of DBC Training is as follows:

Computer Misuse Act 1990: UK law that protects personal data held by organisations from unauthorised access to computer systems and modification of files without consent.
Data Protection Act 1998: Makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Malicious Communications Act 1988: A British Act of Parliament that makes it illegal in England and Wales to "send or deliver letters or other articles for the purpose of causing distress or anxiety". It also applies to electronic communications.

Counter-Terrorism and Security Act 2015: A duty on specified authorities to include the further and higher education sectors to have due regard to the need to prevent people from being drawn into terrorism. This is also known as the Prevent duty.

The Education Act 2002 - Section 157 & 175: Requires local authorities and governing bodies of further education institutions to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children, young people, and adults at risk. In addition, they should have regard to any guidance issued by the Secretary of State in considering what arrangements they may need to make

Keeping children safe in education 2023 This guidance sets out what organisations and agencies who work with children must and should do to safeguard and promote the welfare of all children and young people under the age of 18, including identifying and responding to their needs

Breach of Legislation or Policy

Any suspected breach of this policy may result in DBC Training taking disciplinary action. Serious offences may lead to dismissal and/or possibly prosecution depending on the seriousness and nature of breach

Sanctions Appendix A

Communication Technologies	Staff and other adults				Learners			
	Allowed	Allowed at certain times	Allowed for certain staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile/smart phone may be brought in centre	x				x			
Use of mobile/smart phones in social time		x				x		
Taking photos on a DBC Training issued mobile/smart phones or other camera devices	x				x			
Use of personal email addresses in centre				x			x	
Use of company email for personal emails				x				x
Use of chat rooms/facilities				x				x
Use of personal instant messaging				x				x
Use of social networking sites			x				x	
Use of blogs		x					x	

Sanctions Appendix B

It is intended that incidents of misuse will be dealt with through disciplinary procedures as outlined by the grid below:

Learners	Actions/Sanctions								
	Refer to trainer	Refer to Operations Director	Refer to MD	Refer to Police	Refer to IT support for increased security	Inform parent/carer	Remove internet access	Written warning with actions	Exclusion/ suspension
Accessing material that could be considered illegal		x	x	x	x	x	x		x
Unauthorised use of non-educational sites during sessions	x	x				x	x	x	
Unauthorised use of mobile phone/ digital camera/other mobile device	x	x						x	
Unauthorised use of social networking, instant messaging, personal email	x	x				x	x	x	
Unauthorised downloading or uploading of files	x	x				x	x	x	
Corrupting or destroying data of other users	x	x				x	x	x	
Sending an email, instant message or text that is regarded as offensive, inciting terrorism, harassment or bullying	x	x				x	x	x	x
Continued infringement of above following previous warnings or sanctions	x	x			x	x	x	x	x

Staff/Volunteer	Actions/Sanctions							
	Refer to Line Manager	Refer to Operations Director	Refer to MD	Refer to Police	Refer to IT support for increased security	Disciplinary action Warning	Suspension whilst investigate	Disciplinary action potential to dismiss
Actions which could bring company into disrepute	x	x	x		x	x	x	x
Accidently accessing offensive or pornographic material and failing to report the incident	x	x				x	x	
Deliberately accessing or trying to access offensive or pornographic material	x	x		x	x	x	x	x
Receipt or transmission of material that infringes copyright or Data Protection Act	x	x			x	x	x	x
Excessive or inappropriate personal use of internet	x					x		
Unauthorised downloading or uploading of files						x		
Careless use of personal data transferring data in an insecure manner	x	x				x		
Deliberate actions to breach data protection	x	x				x		
Corrupting or destroying data of others or deliberate damage to hardware of software	x	x			x	x	x	x

Staff/Volunteer	Actions/Sanctions							
	Refer to Line Manager	Refer to Operations Director	Refer to MD	Refer to Police	Refer to IT support for increased security	Disciplinary action Warning	Suspension whilst investigate	Disciplinary action with potential to dismiss
Sending an email, text or instant message during work hours and or using company equipment to send message that is regarded as offensive, inciting terrorism, harassment or bullying	x	x		x		x	x	x
Using social media or personal email to communicate with a learner	x	x						
Using work email to communicate with learner on non-learning related matters and without permission of MD	x	x						
Continued infringements of the above following previous warnings or sanctions	x	x						x

E- Assessment Risk Assessment Appendix C

Could the introduction of apps or additional technology…

☐**... harm the reputation of my institution, or any partner organisation?** *Where there are grounds for judging particular sensitivity or risk, it is important to ensure that there is appropriate consultation before the adoption of the technology. For certainty, it may be beneficial to seek the approval of relevant senior management beforehand.*

☐**... breach the technology's terms and conditions?** *Breach of the terms and conditions of the site will give rise to some level of legal liability, will introduce uncertainty as to whether the use of the tool or site could be withdrawn with disruption to the learners' learning, and may prevent dissemination of what would otherwise be a good example of teaching and learning innovation.*

☐**... put me in a difficult situation if the externally-hosted technology is withdrawn during term?** *Learners may have an action against the institution if their learning is disrupted through the negligence of the institution or its agents, or in breach of a contract. A judgment may need to be made as to the durability of each particular technology. [Intellectual Property Law]*

☐**... lead to any dispute over the ownership of what is going to be created using the technology?** *Particularly in the case of collaboration, or the creation of resources for re-use or with a potential commercial value, it is important to make clear who is to own intellectual property. Particular care will be need where the tutor requires learners to 'hand over' their intellectual property rights to the institution – this may be invalid in law. Copyright in materials created by staff in the course of their employment will belong to the institution, unless there is an agreement otherwise.*

☐**... involve me putting copyright material online without permission or statutory exception?** *The member of staff may be liable for copyright infringement, and the institution liable for the acts of its employee. It may also mean that innovative activity needs to be withdrawn or hidden due to copyright infringement, whereas it could otherwise be hailed as an example of good practice.*

☐**... incite learners to put copyright material online without permission or statutory exception?** *At the very least this will be bad practice and a bad example to set, and it's possible that there might be institutional liability where learners are acting under the direction or instruction of DBC Training.*

☐**... involve the copying of designs, a database or other intellectual property protected resources?** *It's not just copyright and patents. Designs may be subject to intellectual property rights, as might databases. Also, remember that there may be a number of rights involved – a CD involves copyright in the disc's cover, copyright in the musical composition and the lyrics, performance rights, and rights in the recording. These all need to be cleared where relevant, and may not be held by one person or body.*

☐**... lead to details of a potentially patentable invention being made known to the public?** *This could be a very dangerous situation, as a patent will not be granted if details are made public prior to the patent application. A slip in releasing details on a discussion list could prevent*

your institution or a partner body getting a valuable patent, and that could mean a big loss or damages. [Data Protection Law]

☐**... mean that personal information is accessible by unauthorised persons?** *The Data Protection Act 2018 requires your institution to take care of personal information. This could be your learners' personal data, or perhaps research data about other people. In either case, there is a duty only to process or release the data in compliance with the act, and to keep it secure otherwise. Ensure that you treat the personal data with respect, and consider whether the information could be made anonymous instead.*

☐**… require students to sign up to an externally-hosted technology?** *If you let learners know about an IT tool that might assist them, they will have the choice as to whether they submit personal information to that site. However, where you require them to use a technology as part of their course, it may be difficult to say that they have given 'consent' where they'd have to drop out of the course otherwise.*

☐**... involve the holding of external information where public release would be an issue?** *By virtue of freedom of information legislation, institutions must release information held by them upon request, unless non-release is justified by a narrowly-interpreted exception under the legislation. This includes other people's information that you hold, so be careful when sensitive information might be received from third parties, and you don't want to lose their trust. [Liability Issues]*

☐**… be used as a tool for bullying, harassment, or defamation?** *Where the institution is negligent in allowing IT facilities to be used inappropriately, it may be liable for harm to the victim. It is important therefore to set out limits as to permissible behaviour, and to provide moderation and a means for users to complain.*

☐**... leave uncertainty as to what should be done in the case of a complaint being made?** *Where the use of IT technology involves setting up a means for communication, you should ensure that there is a clear mechanism for dealing with complaints, and know what needs to be done if it used.*

☐**... allow the posting, storage, or dissemination of inappropriate and possibly illegal content?** *Where there is the capacity for mischief, you should ensure that you set out what behaviour is acceptable, consider moderation of content, and consider what steps would be reasonable to prevent misuse.*

☐**... prevent the taking down of illegal or inappropriate content under the institution's name?** *Where an IT tool is hosted externally, you may wish to consider whether you have sufficient control over the content should inappropriate use arise, linked with your institution's name. [Accessibility Law]*

☐**... place learners with disabilities at a disadvantage?** *The Disability Discrimination Act 1995 (as amended) places a duty on institutions to be proactive in meeting the needs of users with disabilities. Ensure that any technologies adapted can meet the needs of all users.*

☐**... prevent me from making reasonable adjustments to accommodate particular needs?** *The law requires institutions to make reasonable adjustments to accommodate the needs of users with disabilities. It is best to consider in advance what adaptations could be made to an IT technology to be adopted in order to ensure compliance, and to ensure accessible learning for all*

Flowchart for responding to e-safety incidents Appendix D