DEBUT ACADEMY

2023
V3

E-Safety & Social Media Policy

DEBUT ACADEMY

Introduction

Debut Academy recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within the College, and to support staff and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies.

In furtherance of our duty to safeguard learners and the Every Child Matters agenda, 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 in conjunction with other relevant college policies procedures such as Learner Safeguarding, Internet Use Policy, Anti Bullying Policy, Disciplinary Policy, Code of Conduct and Prevent Policies.

Definition of E-Safety

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable Adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and moderation.
E-safety risks can be summarised under the following three headings.

Content

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

Contact

- Cyber predators - Grooming using communication technologies, potentially leading to sexual assault or child prostitution
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Cyber bullying via websites, mobile phones or other forms of communication device. Emotional abuse that could include blackmail.
- PPI - posting personally identifiable information) - individuals not understanding social boundaries which could put them at risk
- Phishing - cyber security professionals using emails to try to encourage individuals to click on links or other attachments. They may pose as a legitimate company or a relative. They may use 'Smishing' which is sending similar links by email.
- Accidentally downloading Malware to perform harmful actions on a computer

Commerce

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

Scope

The policy applies to all persons who have access to College IT systems, both on premises and remote access. Any user of College IT systems must adhere to e-Safety Rules and our Internet Use Policy. The e-Safety Policy applies to all use of the internet, and electronic communication devices such as e-mail, mobile phones, social networking sites, and any other systems that use the internet for connection and providing of information.

Aims

The aims are to:

- To ensure safeguards on College IT-based systems are strong and reliable
- To ensure user behaviour is safe and appropriate
- To assure that the storage and use of images and personal information on College IT- based systems is secure and meets all legal requirements
- To educate Staff and learners in e-safety and be proactive in alerting them of current risks
- To ensure any incidents which threaten e-safety are managed appropriately

Outcomes

Security

College networks are safe and secure, with appropriate and up-to-date security measures and software in place.

Risk assessment

When making use of new technologies and online platforms, staff are to assess the potential risks that they and their learners could be exposed to.

Behaviour

- It is an unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass, or intimidate another person. This also applies to use of social media systems accessed from College systems.
- All users of technology adhere to the standards of behaviour set out in the Internet Use Policy. All users of IT adhere to College guidelines when using email, mobile phones, social networking sites, chat rooms, video conferencing and web cameras, etc.
- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and learner disciplinary procedures.
- Any conduct considered illegal is reported to the police. Staff must take responsibility for moderating any content posted online.
- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the Lead Safeguarding Manager.
- Staff should keep personal and professional lives separate online Staff should not have students as 'friends' on social media sites that share personal information.
- Staff should be wary of divulging personal details online and are advised to look into privacy settings on sites to control what information is publicly accessible.

- Staff should recognise that they are legally liable for anything they post online. Staff are expected to adhere to the college's equality and diversity policy at all times and not post derogatory, offensive or prejudiced comments online.
- Staff should not bully or abuse colleagues/learners online. Staff entering into a debate with a learner online should ensure that their comments reflect a professional approach.
- Staff should not post any comments online that may bring the college into disrepute or that may damage the college's reputation.
- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of college views, even with a disclaimer, and should consider their postings carefully.
- Staff should not use their college e-mail address to join sites for personal reasons or make their college e-mail address their primary contact method.
- Staff should be aware that any reports of them undertaking inappropriate online activity that links them to the College will be investigated and may result in disciplinary action.

Use of images and video

The use of images or photographs is encouraged in teaching and learning, e.g. recording progress via case studies (before and after treatments), providing there is no breach of copyright or other rights of another person. Staff and learners are trained in the risks in downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example. Debut staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe. Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any material.

Personal information

Processing of personal information is done in compliance with our Data Protection/Privacy Policy. Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual. No personal information is posted to the College website/intranets without the permission of a senior manager. Staff keep learners' personal information safe and secure at all times. When using an online platform, all personal information is password protected. No personal information of individuals is taken offsite unless the member of staff has the permission of their manager. Every user of IT facilities logs off on completion of any activity, or ensures rooms are locked if unsupervised, where they are physically absent from a device. College mobile devices that store sensitive information are encrypted and password protected. Personal data no longer required, is securely deleted.

Education and Training

Staff and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively. Learner inductions and the tutorial programme contains sessions on e-safety. Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages. E-Safety is a topic within the learner FOCUS BOOK.

Learners know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. In classes, learners are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

Learners are encouraged to embrace ICT equipment during lessons and they will sometimes use Debut laptops or tablets or their own phones to research. Tutors will actively monitor use of equipment at these times to ensure learners are (a) doing the task that has been assigned and (b) they are not accessing any sites that have no relevance to their learning or others that may put them at risk.

Debut will ensure that its ICT equipment has appropriate Malware and Anti-Virus software so that risks are minimalised with data storage. Laptops and tablets are checked yearly for servicing and updating any necessary software. Posters alerting the e-safety risks and appropriate online behaviour are displayed in training rooms and other rooms that is for computer use.

Incidents and response

A clear and effective incident reporting procedure is maintained and communicated to learners and staff. Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring. Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected learners, etc.

Responsibilities

Maintaining best practice in IT procedures and practices to manage any e-safety risks effectively is paramount.
The following are responsible for implementing it:-

Staff

Designated Safeguarding Lead for all e-safety matters in relation to College Learners.
Contract Managers for championing good e-safety practice in College IT facilities and processes, and for providing technical expertise when issues are being investigated.
Student Liaison Officer for providing pastoral and practical support for learners dealing with issues related to e-safety and for incorporating e-safety in learner induction, supporting the tutorial scheme of work, and for providing an appropriate range of resources to tutors.
All tutors for embedding e-safety education and practice into the learner's programme.
All Staff for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility and staying alert to any risks, reporting any concerns promptly to the Safeguarding Lead.

Education and Training

With the current unlimited nature of internet access, it is impossible for Debut to eliminate all risks for staff and learners. It is our view therefore, that the College should support staff and learners to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively. Learners are encouraged to participate in Wider Curriculum weeks where e-safety and online risks is a regular topic.

E-Safety & COVID

- Learners will receive e-safety guidance, expectations and rules regarding attending zoom training online during their inductions. Learners are informed they must have their camera and audio on at all times.
- During times when Debut is under lockdown a continuous record of learner attendance on zoom weekly lessons is kept and the designated Contract manager will follow up any absences, this is to ensure that learners safeguarding is paramount and there is a valid reason for non-attendance.
- Zoom non-attendance should not be ongoing as it is vital that during non-face to face training contact with all learners is regularly maintained to ensure their wellbeing and safety is known.
- Learners who will refuse to turn on their camera during zoom group lessons will receive a follow up 1:1 zoom meeting with their tutor to check wellbeing and will be encouraged to have their camera on during their future lessons. Tutors are advised to report any areas of concern regarding learners safeguarding during remote learning to the Safeguarding Officer. If learners fail to comply with zoom rules they will be transferred to onsite lessons.

E-Safety & Online Exams

During COVID some NVQ exams are conducted online remotely following the Awarding Body's strict guidelines. Linda Edwards (Center Invigilator) is solely responsible for overseeing all remote online exams.
Linda is also the company DesignatedSafeguarding Lead and is fully aware to ensure that wellbeing is at the forefront of conducting online exams and following up any concerns.

For Learners

Learners will complete an e-safety e-learning workshop, so they know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly. Appendix A shows E-Safety Guidelines and Appendix B shows Guidelines for Students (Social Media)

For Staff

Staff will take part in mandatory Safeguarding training (which includes e-safety) with updates every 3 years. This will be monitored by the Safeguarding and HR Officer and will take the format of a updates at meetings, PowerPoint workshop which allows tutors hands-on experience.

Appropriate Monitoring & Filtering

What is a filtering system?

This system blocks access to harmful sites and content. Monitoring systems: identify when a user accesses or searches for certain types of harmful content on college devices. Your school is then alerted to any concerning content so they can intervene and respond.

Debut have appointed an outside company to set up a DNS System.
This sits on the internet connections and devices and can pick up key words that have been pre-set into it to flag a search or visit to a web page. It also allows the college to block specific website URLs (e.g. unsuitable forums, sexual sites, terrorist sites).

This system works via a piece of software being installed onto IT equipment that is included in the monitoring process. It will provide full visibility on Debut equipment and we can see which device conducted a 'specific' search that may need following up. If someone with IT knowledge tries to disable the system Debut will receive an alert. Specialised software is uploaded to Debut devices (used by staff and learners) so that they can be monitored for any web searches and will relay information to the filtering searches provided.

Filtering and blocking unsuitable or concerning web searches is limited to the devices used. For example, if a learner uses their own mobile phone for research via Debut internet the blocks for specific URLs will be in place. These are not in place if they use their own 4G or 5G internet, however, tutors will be responsible for managing and overseeing research tasks in class to minimise risk. When filtering reports are accessed we will only be able to identify via Debut IT equipment as it will have a known identity. This will not be the same when a search via Debut internet facilities is conducted by a mobile phone (the identity remains confidential for data protection purposes).

Debut will keep records (as accurately as possible) of users who access Debut identifiable IT equipment (date and time) so that if any concerns are raised the DSL or Deputy Safeguarding Staff member can have a 1:1 meeting with the individual to look into the matter fully with them, logging the process on a filtering log.
If the filtering system flags that a specific amount of mobile phones has accessed a URL that may be a concern, the DSL will consult the SOWs for that day or Tutors who have conducted lessons to determine if they were delivering a specific 'focus topic' or asking learners to research in class. If a tutor finds that they would like learner(s) to access a URL that is blocked (because of a keyword) the tutor can look at the webpage and check it is suitable for access and provide a one-time access code to gain viewing by the learner(s).

If a filtering report flags a search on a URL that may be of a concern, the DSL or Deputy will look at the webpage content to determine if there is anything that could potentially be harmful or a safeguarding risk. If it constitutes a risk then the URL will be blocked. The staff member will

Debut will also have designated browsers that are connected to 'Safe Search' which will provide another level of security. Debut will appoint designated staff to monitor and run filters to obtain reports on web searches conducted via Debut internet sources. The responsibility to monitor reports and filtering will be undertaken by:

Linda Edwards - Designated Safeguarding Lead & Centre Manager
Kersti Harding - Safeguarding Deputy & Centre Manager Brentwood

Incidents and Response
Where an e-safety incident is reported to Debut the matter will be dealt with very seriously. The College 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, Senior Manager, the College Safeguarding Officer or the Centre Manager. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the College will review what has happened and decide upon 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. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Checklist:
Impact on Learners/Staff: Provide College learners and staff members a safe online environment.
Impact on Diversity: This is an inclusive policy and covers e-safety issues involving hate and intolerance.
Impact on PREVENT: This policy highlights the dangers of radicalisation through websites and social media
Impact on Health & Safety: Provide a safe online environment for Staff and learners
Impact on Privacy/Data Protection/Freedom of Information: Outlines staff and learner guidelines for protection of personal data online.

Responsibility and Authority
The organisation has ultimate responsibility for e-safety learner protection and will ensure that the arrangements for safeguarding learners are effective, robust and reviewed on a regular basis. As such at Debut have assigned the following staff member to oversee e-safety.

Linda Edwards
Safeguarding Lead
01268 560552 or 07774 096187
linda@debutacademy.com

Scams & Online Risks

The Designated Safeguarding Lead will regularly provide bulletins to disseminate information relating to current scams and online risks. This information is brought together from various sources, e.g.

Police Newsletters
Which Scam Advice
Direct.gov Scams
Social Media

Debut is committed to ensuring that their staff, learners and employers are made aware of any risks online to increase awareness, including how to report scams, how to avoid phishing scams and how to recognise them.

Debut also remind their staff, learners and employers of the 10 tips for staying safe on the internet:

1. Keep personal information professional and limited.
2. Keep your privacy settings on.
3. Practice safe browsing.
4. Make sure your internet connection is secure.
5. Be careful what you download.
6. Choose strong passwords.
7. Make online purchases from secure sites.
8. Be careful what you post.
9. Be careful of who you meet online
10. Keep your anti-virus up to date.

Bulletins are uploaded on the Padlet information areas, posters in classrooms and on Announcements WhatsApp Chats.
Debut Managers also perform knowledge checks in classes to check learner's awareness of e-safety and remind them to look at bulletins.

Please refer to Debut's linked policies below for additional information regarding E-Safety standards:

Anti-Bullying, Anti-Harassment and Victimisation Policy
Code of Conduct – Staff Policy
Code of Conduct – Learner Policy
Complaints Policy
Counselling Policy
Confidentiality and Disclosure Policy
Privacy Policy
Disciplinary Policy
Employer (Work Based) Support & Expectation Policy
Equal Opportunities & Inclusion Policy
Freedom of Information Policy

Guidance Policy
Health & Safety Policy
Health & Wellbeing Policy
Induction Procedure – Staff Policy
Induction Procedure – Learners Policy
Internal Quality Assurance (IQA) Policy
Internet Use Policy
Learner Support & Super Group Policy
Learner Safeguarding & Safeguarding Vulnerable Adults Policy
Learner Positive Behaviour Management Policy
Learner Contribution & Learner Voice Policy
Lone Worker Policy
Meetings Policy
Mentoring – Staff Policy
Mentoring – Learner Policy
Observation of Teaching, Learning & Assessment Policy
Prevent Duty Policy
Quality Assurance Policy
Safer Recruitment Policy
Staff CPD/Personal Development Training Policy
Staff Confidentiality Policy
Teaching & Learning Policy
Whistle Blowing Policy

Policy Revision
Issue 06 - Updated June 2024
Revision Date – June 2025