DEBUT ACADEMY

2023
V3

# Appropriate Use of Technology Policy

DEBUT ACADEMY

## Introduction

Debut Academy is committed to making sure that our learners have access to IT equipment for their study needs, which includes access to e-learning and the internet. We are keen to encourage learners to use our facilities to improve their learning and achievement throughout their learning experience, and this extends to ICT skills.

## Policy Statement

The internet is a large global network, providing information which can help with study. However, Debut needs to ensure that the information that is researched or accessed for is acceptable. We need to take steps to monitor the usage of the internet by learners. The internet is not controlled by any one organisation and you cannot always be sure of the standard of information on the internet.

Debut Academy has a responsibility to safeguard its learners, and also make sure that the information that is used by them and others does not break any laws and abides with our policies such as (but not limited to) our Equality and Diversity, Code of Conduct, Data Protection & GDPR, AI, E-Safety & Social Media and Safeguarding.

## Scope of Policy

Debut Academy's computers can be used to access the internet for legitimate reasons which are related to course or work duties. This may involve research to complete assignments, accessing information to support learning, e-testing, e-learning and personal development/support courses.

## Staying Safe Online

1) Don't use lazy passwords

If your account is hacked, it's often because someone has worked out your password. Never use a password that anyone could guess or work out - a middle name, pet's name or favourite football team. Include capital letters, numbers, symbols and punctuation in your password for extra security. So if your pet is called Hamish, try using the password Ham15h! And never use the same password for different accounts. That will mean when people can get into one of your accounts, they can access everything!

2) Be careful what you post online

Everything you write on a social network is public, so don't give out any personal details, such as your address, bank details etc. That would be the equivalent of shouting the details out of the window. Don't advertise online that you are going on holiday, as that leaves you vulnerable to burglars. Many employers also google prospective employees before hiring, so don't post anything that could damage your chances of getting a job.

3) If you are a victim of cyberbullying, do not answer back

The rule for dealing with cyberbullies is to "**stop, block and tell**". Don't answer back, as that will only feed the abuse, block the person or message and tell someone you trust and report it to the police.

4) Never open email attachments or click on links from strangers
Viruses are often spread via attachments on emails, so if you do not know what an attachment is about, **do not** open it. Never open .EXE attachments.
The same is true of links. Even if it looks like a safe link, it may be forwarding to somewhere you weren't expecting.

5) Watch out for email scams
Spoof emails are very common, ranging from Nigerian princes asking for a short-term loan to proper-looking companies asking you for personal information. This is called phishing. If you get an email from someone like a bank, eBay or PayPal, saying there is a problem with your account, forward it to the company in question to get confirmation it's from them. Most companies will never ask you for your password. Try searching on google for similar scams to check if you are uncertain. Keep up-to-date with the latest scam news from Debut Bulletins issued monthly.

6) Even emails from friends can be suspicious
Robert Fox, a journalist for the Evening Standard, told of how his email contacts were all sent an email saying he was stuck in Cyprus after having his passport and wallet stolen and asking for money. Some of his friends did this. All of this was done when a hacker got into his account, changed passwords and locked him out.

7) If you're using online banking, use all the banks security recommendations
Many banks will recommend adding a piece of software which guards against hackers. **Do it**. That will give your account maximum protection. For example, HSBC uses a programme called Rapport. Only complete online transactions where the URL starts with 'https' and not just 'http'. **The 's' stands for secure**. Do not complete internet banking on computers that may be infected. Again, remember your bank will never ask for your login details via email, text or phone.

8) If you get hacked, change your password immediately
Often, when you are hacked, a spam email will be sent to all your contacts. If you find out this has happened, change your password to something completely different immediately. Alert the people that may have received a spam email from your account to delete it immediately without opening it.

9) Read the small print
When you're signing up for an account, make sure you look for the box near the bottom, which asks if you want to receive more information. Some require you to tick them to opt-in, some require you to tick them to opt-out, so read it carefully. Only fill in the mandatory boxes, marked with an asterisk *. Some companies will sell your personal data, so make sure you take time to tick/untick the right boxes.

10) Use a firewall, anti-virus programme and anti-spyware program
You can use Windows' own firewall, or a third-party, such as Norton or McAfee. **But make sure you don't use both as they can interfere with each other.**
- A firewall will stop unauthorised people hacking on to your computer.
- Anti-virus programmes will guard your computer from viruses which could destroy your computer.
- Anti-spyware will look out for programmes such as keyloggers and trojans which spy on your computer use in an attempt to learn passwords or account details.

**Rules & Expectations at Debut**

In order to safeguard our learners, we must have rules in place and for this reason they must NOT use Debut's IT systems/equipment for the following:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Debut email service (whether it is a Debut designated learner/staff email or a personal email.
- Downloading, creating or sending to others information or images or other material that may threaten, harass or discriminate against anyone else.
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Downloading or creating material that is not directly related to a person's course, study or job role.
- Doing things deliberately that wastes staff time and effort or disrupts other learners, destroys or damages other people's data and information.
- Accessing security systems on computers to change any restrictions imposed by Debut, such as specific internet sites or preferred search engines.
- Stealing, using, or disclosing someone else's password without authorisation.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorisation.
- Sharing confidential material, trade secrets, or proprietary information outside of the organisation.
- Hacking into unauthorised websites.
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.
- Introducing malicious software onto the company network and/or jeopardising the security of the organisation's electronic communications systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organisation.
- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection.

**Staff Computer, email and internet usage**

- Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted.

- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.
- All Internet data that is composed, transmitted and/or received by Debut's computer systems is considered to belong to Debut and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
- The equipment, services and technology used to access the Internet are the property of Debut and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by Debut if they are deemed to be harmful and/or not productive to business
- The installation of software such as instant messaging technology is strictly prohibited without prior approval
- The use of internet for personal use during working hours is strictly forbidden and staff may be disciplined if they are found to be in breach of this.
- Staff must adhere to any password changes that are scheduled in order to maintain security throughout its operations.

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification.

### Clear Desk and Clear Screen Procedures

In order to reduce the risk of unauthorised access or loss of information, Debut enforces a clear desk and screen procedures as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.
- To back up important Debut files regularly on separate hard drives or on the share drive facility.
- Staff should adopt the same protocols when using SMART screens in classrooms - e.g. logging into their emails or using other portals - all must be logged out after use and equipment turned off.

### E-Safety for Learners

Debut learners will complete ETF courses relating to e-safety at commencement of their course (gaining certification of completion). Additional e-safety guidance is provided in learner's Focus Topic Book, during Wider Curriculum weeks and via safeguarding bulletins and knowledge checks.

## Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Debut's offsite working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
- Mobile Storage Devices Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.
- Only Debut authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.
- Employees must use only software that is authorised by Debut on Company computers.
- Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Debut's computers must be approved and installed by Debut administration staff.
- Computer equipment loaned to staff to carry out their duties must be used in accordance with this policy and kept safe and secure at all times.
- Any misuse of loaned equipment will be subject to disciplinary action. Staff must not leave any loaned IT equipment in a vulnerable situation that would cause it to be stolen or damaged or they will be subject to its replacement or cost of repair.

## Actions upon Termination of Contract

All Debut equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Debut at termination of contract. All Debut data or intellectual property developed or gained during the period of employment remains the property of Debut and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering data that is created and stored on Debut computers is the property of Debut and there is no official provision for individual data privacy, however wherever possible Debut will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

## Breaches

Debut has a zero tolerance to any breaches of the aforementioned guidelines. Breaches will be dealt with in accordance with its company Disciplinary policy.

## Monitoring

Debut has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000. Debut have appointed SJ Systems who provide filtering DNS software on their devices - this is in place for the following reasons:

- To intercept and block phishing scams
- To intercept and block malware
- To monitor URL searches to alert the DSL of any safeguarding-related topics.

Please be aware that Debut have blocks in place on specific keywords - when used in URL searches these will be blocked.

## Reporting Breaches

It is the responsibility of all staff and learners report suspected breaches of this policy without delay to your supervisor/assessor or line management. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Debut's disciplinary procedures.

## Helplines & Advice

The following contact information may be accessed if a learner or staff member require confidential support and advice on specific issues such as cyber bullying, harassment and online stalking:

REVENGE PORN HELPLINE
Phone us: 0845 6000 459
Email us: help@revengepornhelpline.org.uk
Visit our website: www.revengepornhelpline.org.uk

CHILDLINE
http://www.childline.org.uk
Tel: 0800 11 11

INTERNET MATTERS
http://www.internetmatters.org/
Email: info@internetmatters.org

GET CONNECTED
http://www.getconnected.org.uk/
Freephone 0808 808 4994

NATIONAL BULLYING HELPLINE
http://www.nationalbullyinghelpline.co.uk
Email admin@nationalbullyinghelpline.co.uk
Tel: 0845 22 55 787

E-SAFETY TRAINING.ORG (2JOHNS)
http://www.esafetytraining.org

VICTIM SUPPORT
www.victimsupport.org.uk
Tel: 08 08 16 89 111

## E-Safety & Social Media

Debut has a separate policy for e-safety and social media, please refer to this for further information. Debut also provides a workshop on this subject to educate our staff and learners on keeping safe online and recognising any risks

Please refer to Debut's linked policies below for additional information regarding Appropriate Use of Technology 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
E-Safety & Social Media Policy
Privacy Policy
Disciplinary Policy
Employer (Work Based) Support & Expectation Policy
Equal Opportunities & Inclusion Policy
Freedom of Information Policy
Health & Safety Policy
Health & Wellbeing Policy
Induction Procedure – Staff Policy
Induction Procedure – Learners 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
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