Digital Safety Policy

Written by:	IT Services Manager
CLT Sponsor:	Director of Estates and IT
Consulted with:	Director of Student Services, Director of Teaching, Learning and Development, Head of Marketing and Communications, DPO and Compliance Manager
Next Review Date:	Oct 2024
Version:	Oct 2022

1. Purpose and Scope

1.1 Exeter College recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

1.2 Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In furtherance of our duty to safeguard learners and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care.

1.3 This policy must be read in conjunction with other relevant College policies including the Child Protection and Safeguarding Policy, the Data Protection Policy, the Anti Bullying Policy, the CCTV Policy, the Staff Code of Conduct and the Learner Code of Conduct.

1.4 This policy applies to all internet use and forms of electronic communication.

1.5 It applies to the use of technology on and off Exeter College premises.

1.6 This policy applies to all staff, governors, students, parents, and any visitors on Exeter College premises, including residential accommodation.

1.7 All staff and students, governors, and visitors agree to the 'Exeter college IT terms of use', when logging on to College IT Services network.

2. Policy

2.1 Monitoring usage

2.1.1 Exeter College actively monitor, log and report on learners and staff use of IT systems and IT network usage as part of the College's responsibility towards the 'safeguarding of young people and vulnerable adults' and Prevent duty for terrorist and extremist behaviour.

2.1.2 An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the College's disciplinary process.

2.1.3 Any use of college resources or online communication considered to be unlawful will be reported and shared with the Police for further investigation

2.2 Cybersecurity

2.2.1 Exeter College IT systems and the College's Information Security Management System is certified to meet the Cyber Essentials (registration number IASME-CE-038621) Information Security and Cyber Security standards.

2.2.2 These standards are regularly reviewed by independent experts providing staff, learners & stakeholders reassurance that Exeter College IT systems cybersecurity follow the highest levels of best practice.

2.2.3 Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring/accessing someone else's digital identity is a criminal offence and will be referred to the college's disciplinary procedure.

2.2.4 If there are any concerns or anything suspicious is noticed in regards to the cybersecurity on the Exeter College network or systems the IT Helpdesk on 01392 400497 should be contacted.

2.3 Communication between staff and learners

Staff must ensure that

2.3.1 They establish safe and responsible online behaviours.

2.3.2 Communication between students and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, webcams, websites and blogs.

2.3.3 They do not share any personal information with a student.

2.3.4 They must not request, or respond to, any personal information from a student other than that which might be appropriate as part of their professional role.

2.3.5 All communications are transparent and open to scrutiny.

2.3.6 They are circumspect in their communications with students to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

2.3.7 Their personal social networking sites should be set to private, and students are never listed as approved contacts unless specific authority is given by an Assistant Principal to meet a course or programme specification.

2.3.8 They will never use or access the social networking pages of students.

2.3.9 Staff must not communicate with learners from non-College accounts or personal phone numbers.

2.4 Social Networks

2.4.1 The College uses social networks including Facebook, Instagram and Twitter to share information and gather opinions from its stakeholders including students, parents/carers, customers and local residents. The College social media sites are monitored by a member of the marketing team and inappropriate material, or comments are passed to the appropriate person on the Senior Leadership Team if there are any concerns.

2.4.2 Social media sites can be valuable educational resources. They can, for example, be used to foster twinning relationships with overseas schools or colleges. Exeter College takes the view that social media sites should not be blocked but that students should be educated about their safe use.

2.4.3 Student usage of social networks in lessons and other college facilities, which disturbs their concentration, that of others or blocks computer usage, is managed by lecturers and other staff appropriately and in line with agreed behavioural rules, which maximise student success. These rules are likely to include not using social media sites unless they are integral to the lesson content. It is expected that tutors and lecturers would utilise the Conduct and Support Procedures for persistent misuse.

2.4.4 Bullying or other inappropriate use of Social Media sites is a disciplinary offence for students and staff. IT Services will assist and advise in IT Services-related disciplinary investigations – please see 'Code of Practice on the use of Social Media' for further information regarding staff use of social media.

2.5 Use of Images and Video

2.5.1 The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g., images rights, or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

2.5.2 Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. No image/photograph owned by Exeter College can be copied, downloaded, shared, or distributed online without permission from the Head of Marketing and Communications. Photographs of activities on college premises should be considered carefully and have the permission of the Head of Marketing and Communications before being published. Approved photographs must not include names of individuals without their explicit consent.

2.5.3 Where the capture of images of students and groups have been authorised, this must be done using College media equipment only or with prior approval for any external media organisation.

2.5.4 Images taken are subject to the data retention schedule. Staff need to remain sensitive to any student who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings. Staff must never take photographs of learners for their personal use. Images will be securely stored on college owned devices and used only by those authorised to do so.

2.6 Personal Data and Data Protection

2.6.1 Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018.

2.6.2 Staff must ensure that they comply with the college's Data Protection Policy and associated processes and procedures.

2.7 Security

Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent or mitigate accidental or malicious access of college systems and information. Digital communications, including email and internet postings, over the college network, will be monitored in line with the Information Security Policy.

3. Implementation

3.1. Role and responsibilities

The reporting responsibilities for digital safety follow the same lines of responsibility as the College Safeguarding.

3.1.1 All Staff & Workforce must

- Be responsible for ensuring the safety of learners
- Report any concerns or disclosures immediately to the Designated Safeguarding Lead (DSL)
- Never offer assurance of confidentiality everything discussed must be reported
- Keep to the terms and conditions of the Acceptable Use of IT Services Agreement (Appendix 2) at all times
- Attend staff training on e-safety and display a model example to learners at all times.
- Actively promote good e-safety practice.
- Communicate with learners professionally and in line with the college policies and procedures at all times and adhere to the staff code of conduct
- Have an up-to-date awareness of digital-safety matters and of the Digital Safety Policy.
- Ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Be aware of digital-safety issues related to the use of mobile phones, cameras, and handheld devices and that they monitor their use and implement current Exeter College policies with regard to these devices.
- Act as good role models in their use of IT Services, the internet, and mobile devices.
- Always take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Ensure they transfer data using encryption and secure password protected devices.
- Ensure they encrypt and password protect personal data, which is stored on any portable computer system, USB stick or any other removable media.
- Use devices capable of being password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- Use devices which offer approved virus and malware checking software.
- Securely delete data from the device, in line with Exeter College procedure (Appendix 1) once it has been transferred or its use is complete.

3.1.2 Learners must

- Keep to the terms and conditions of the Acceptable Use of IT Services Agreement (Appendix 2) at all times.
- Receive appropriate e-safety guidance as part of their programme of study.
- Inform a member of staff where they are worried or concerned an e-safety incident has taken place involving them or another member of the college community.
- Act safely and responsibly at all times when using the internet and/or mobile technologies and adhere to the Exeter College Computer Network Terms of use for students

3.1.3 Safeguarding Leads (DSL and DDSL) must

- Lead the Safeguarding Steering Group

- Call e-safety meetings when required
- Ensure appropriate delivery of staff development and training
- Record incidents
- Report any developments and incidents to the Senior Leadership Team
- Liaise with the local authority and external agencies to promote e-safety within the College community
- Receive weekly prevent reports from IT Services that monitor user content with regards to extremist websites. Where a student or staff member has attempted to view extremist content using the college system they will be spoken to by a member of the safeguarding team and a proportionate decision will be made on how to proceed. This may range from offering support through our welfare team to referring the individual to Prevent.

3.1.4 IT Department must

- Ensure the College's IT infrastructure is secure and meets best practice recommendations
- Ensure IT security incidents are recorded, investigated and resolved within reasonable a reasonable timescale
- Report any e-safety concerns or disclosures immediately to the Designated Safeguarding Officer (DSL)

3.1.4 Exeter College will ensure that staff and students are allocated passwords to the system by IT Services. The college password policy is defined as part of the Information Security Policy

3.2. Training and guidance

3.2.1 All Staff

- Will receive an induction which includes an introduction to working systems/ environments and digital learning. All staff are aware of the references to digital safety in the staff code of conduct
- Are required to attend annual safeguarding training, including update training, to maintain an understanding and awareness of online sexual abuse and harassment
- Engage with mandatory training on Safeguarding, Data Protection and Cyber-Security at least every two years. Records of staff training are managed and update by The People Team.

3.2.2 Learners

- Will benefit from tutorial planning, which includes appropriate and relevant guidance on Safeguarding, Digital Safety, Data Protection and Cyber-Security.
- Will be aware of The Student Hub Sharepoint page include online guidance for safeguarding, including how to report concerns and key definitions for sexual abuse and harassment.
- Will receive guidance on what precautions and safeguards are appropriate when making use of specific the internet and mobile technologies from their curriculum tutor.
- Will be prompted with a reminder of the Colleges IT acceptable use each time they log in to a Exeter College Computer.
- Will benefit from tutorials which highlight the college e-safety expectations and e-safety themes will be part of awareness campaigns throughout the academic year.
- Are made aware of digital safety through the Exeter College Computer Network Terms of use for students included in their eILP.

3.3 Publishing Material Online (inc. images of learners)

Whilst we wish the college's website to be a valuable tool for sharing news, information and promoting achievement with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be considered:

- Consent should be sought from the individual before any image is uploaded, if that is the legal basis we rely on. Learners need to be made aware that their image could be visible for a certain length of time, so that the consent given is "informed" in line with the UK GDPR.

- If an image/audio/video recording of a student under 18 is used, then they should not be named (including in credits) and ideally young people should not be on their own.
- Files should be appropriately named.
- Only images of students in appropriate dress should be used and group photographs are preferred in preference to individual photographs.
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Material should be proof-read (e.g., to check for spelling or grammatical errors) before being published.

4. Associated Documentation

4.1. This policy should be used in conjunction with the following policies:

4.1.1 Child Protection and Safeguarding Policy
4.1.2 Information Security Policy
4.1.3 Data Protection Policy
4.1.4 Data Retention Schedule
4.1.5 Social Media Policy
4.1.6 Plagiarism and Malpractice Policy

4.2. This policy should be used in conjunction with the following procedures and other documentation:

4.2.1 Staff Code of Conduct
4.2.2 Student Code of Conduct
4.2.3 Code of Practice on the use of Social Media
4.2.4 Exeter College Computer Network Terms of use for students
4.2.5 Administrators follow Administrators' code of conduct
4.2.6 IT Services Acceptable Use Agreement (appendix 2 below)

4.3. Associated Legislation

4.3.1 Data Protection Act 2018
4.3.2 Freedom of Information Act 2000
4.3.3 Computer Misuse Act 1990
4.3.4 Regulation of Investigatory Powers Act 2000
4.3.5 Privacy of Electronic Communications Regulations 2003
4.3.6 UK General Data Protection Regulation (UK GDPR)
4.3.7 The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
4.3.8 Keeping Children Safe in Education (latest version)

5. Monitoring, Review and Evaluation

5.1 The Senior Leadership team is responsible for the approving of the Digital Safety Policy
5.2 The Board (Quality and Standards Committee) is responsible for adopting the Digital Safety Policy.
5.3 Exeter College is committed to complying with the law in respect of Safeguarding, Data Protection and Digital Safety matters.
5.4 The IT Services Manager is responsible for the maintenance, review and monitoring of the Digital Safety Policy and will conduct a bi-annual review.
5.5 The definitive version of the policy is stored in the College Leadership SharePoint Site

Appendix 1 - BYOD – Bring your own device

Introduction

Bring your own device (BYOD) is the practice of allowing staff to use their own devices in the workplace and to use those devices to securely access the organisation's systems, applications and information. This can mean using their own smartphones, tablets or laptops for work.
BYOD is optional and offered to provide greater flexibility. It may not be available to all staff.

Do

- keep your passwords secure
- use biometric features to secure the device if possible
- keep your operating system updated
- be careful who can see your screen when accessing work systems
- report lost or stolen devices
- be aware of your responsibility for all costs
- help IT to conduct spot checks if required
- immediately inform IT Services if your device is lost or stolen

Don't

- share your device or passwords
- make copies of data or take screenshots
- access systems without authorisation
- save work in unapproved locations or applications

Supported devices

Due to the rapid pace of change it is not possible to support BYOD on all devices. BYOD will only be permitted on devices which can run the latest version of the Apple or a supported version Android operating system. Staff will be expected to make sure their devices are kept updated or risk losing access to some systems.

Devices must be encrypted and have passcode or biometric security if available with a reasonable timeout to lock automatically. Jailbroken or rooted devices are strictly prohibited. Staff must not circumvent security controls.

Access

- Devices may connect Eduroam Wi-Fi but are not permitted to connect directly to the corporate network.
- Use of BYOD and access to corporate systems is subject to other organisation policies and practices and does not override or supersede them.
- BYOD is optional and may not be appropriate in all roles.
- The organisation reserves the right to revoke access if staff do not follow this policy.

Responsibilities

- Staff may only connect to organisation systems for the purpose of authorised work.
- Use of a device that has access to work systems by BYOD should be limited to its owner and must not be shared.
- Devices must be maintained as stated in the 'supported devices' section.
- You should always keep your account log in details, passwords and pins confidential and never share them with anyone.

- Staff should be conscious of the setting in which devices are being operated and should ensure data and systems displayed are not visible to others. Data accessed must not be saved to the device or copied off it. Screenshots of systems must not be taken.

Loss or damage

- The organisation will not accept any liability for loss or damage of personal devices and data that are using the BYOD system.
- Staff should inform IT immediately if they lose their personal device or have it stolen. IT will attempt to remotely wipe or disable the device.

Acceptable use

- Only use the BYOD policy to access work systems during working hours.
- Only access systems which they require and normally use.
- Never try to access systems for which they are not authorised.
- Confidential data must only be accessed for a specific work-related requirement.
- Any suspected breach must be immediately reported to IT.

Costs

- Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.
- Staff are responsible for all mobile data or Wi-Fi hotspot costs related to BYOD usage and should monitor these to ensure they have sufficient allowance.

Monitoring

- The organisation will monitor usage of BYOD devices from time to time including the make and model of devices in use and the version of the operating system currently installed. Where operating systems are found to be out of date the staff member will be informed and expected to upgrade to the most current version within 5 days.
- Failure to remediate will result in access to BYOD services being withdrawn.
- Spot checks on BYOD devices may be initiated at any time and staff will be expected to allow access to authorised personnel to check settings related to BYOD usage. Spot checks will always be conducted in the presence of the staff member and devices will never be taken away from their owner.
- Technical support personnel can access details on usage of corporate applications via the BYOD system but cannot access personal application data. In some instances, device location may be collected but this data will only be used if the device is lost or stolen.

Digital equity

The organisation is committed to digital equity. All systems accessible through BYOD are also available on the corporate network and computer system.

Appendix 2 - Acceptable Use of IT Services Agreement

The Acceptable Use Agreement is to ensure that:

- Staff are responsible users of the internet, social media, email, and other recreational use.
- Our digital systems (email, Facebook, website etc.) are protected against hacking of all descriptions.
- Devices are protected against malicious action.
- Data is protected and access is allocated on a least privilege basis.

Acceptable use policy agreement

- I understand that I must use IT Services in a responsible way, protecting my safety, the safety and security of the IT Services and Students.

Professional and personal safety

- I understand that the College will monitor my use of IT Services, emails, and other forms of digital communication.
- I understand that the rules set out in this document apply to IT Services both inside and outside the College.
- I understand that the College IT Services are provided for educational purposes only.
- I will not disclose my username or password to anyone else nor will I try to use any other's username or password.
- I will immediately report any illegal, inappropriate, or harmful material or incident to the safeguarding team.

Professional communications and actions when using the College's IT Services

- I will not access, copy, remove or otherwise alter any other user's files, without consent.
- Avoiding the use of aggressive or inappropriate language, I will communicate with others in a professional and courteous manner. I will be tolerant and respectful of the views of others.
- I will only use chat and social networking sites in accordance with the College's digital safety policy.
- I will not engage in any on-line activity that will compromise my profession or bring the College into disrepute.
- In the event of a data breach, I will report immediately to the Data Protection team.
- I will follow the College's guidance, set out in the Digital safety policy.

Safe and secure access and storage

- The College has a responsibility to offer safe and secure access to digital technology. I agree to report any deficiencies in the IT Services to the Data Protection team.
- I will pay particular attention to:
- a) phishing
- b) downloading insecure attachments to emails
- c) concealing usernames and passwords (login details)
- d) downloading software without permission (the danger of malware and viruses).
- Because of the danger of malware and viruses, I will not open any attachments unless the source is known and trusted.
- I will not upload, download, or access any material which is illegal (child sexual abuse images, racist material, adult pornography…) or inappropriate or might cause harm or distress to others.
- I will not use any software designed to work around the College's firewall or anti-virus programs.
- I will not install any programs or alter the settings on any computer without express consent from IT Services via the new software procedure.
- I will not damage or disable any of the College's IT Services equipment or equipment belonging to others.

Data protection

- I will not transport, hold, disclose, or share personal information as set out in the College's Data Protection Policy. Externally exported personal data must be encrypted.
- I understand the necessity of keeping private any personal data, except when required by law to disclose such to the Designated Safeguarding Lead (DSL) or another appropriate authority.

- I understand that safeguarding trumps data protection. When children are suffering from, or may be at risk of, suffering significant harm concerns must always be shared with children's social care or the police.