Digital Safety Policy

Written by:	Jennie Hamilton and Nick Couzens
CLT Sponsor:	Jennie Hamilton
Consulted with:	Nick Couzens, Tammy East, Richard Brine
Next Review Date:	September 2020
Version:	September 2018

1 Purpose

Exeter College recognises the benefits and opportunities which new technologies offer to teaching and learning. 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 within the college 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 and Keeping Children Safe in Education 2018, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

2 Definitions

Mobile Technologies	Any mobile device owned by the College or by an individual student or member of staff
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation

3 Policy

The policy applies to all members of the college community who have access to the college IT systems, both on the premises and remotely**, including residential accommodation**. Any user of college IT systems must adhere to the Code of Practice for the Acceptable Use of ICT and Electronic Communications Systems.
The Digital-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile technology; messaging and social media sites.

3.1 Practices to Promote Digital–Safety

With the current unlimited nature of internet access, it is impossible for the college 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

3.1.1 Induction

- Students and staff will receive an induction to the College's ICT systems and resources when they join the College, including the College's portal and Moodle site
- Staff will be inducted into the complete MIS site and their faculty /department portal sites
- Students will receive induction into the student MIS pages and their own student faculty pages
- All students agree to the 'ICT Acceptable Use Policy', when they first log on to the College ICT network.

3.1.2 Passwords

Staff and students are allocated passwords to the system by ICT Services. They are forced to change their password to a memorable and complex one when they first log on. Guidance is given on the use of strong passwords. The system is set to require passwords to be updated every 59 days for staff and students.

3.1.3 Safeguarding Training

Staff training on safeguarding is compulsory for all members of staff at Exeter College as is the requirement to have updated training every 3 years. Staff also receive regular updates through the Student Experience Bulletin and other training and staff development opportunities. Safeguarding training includes updates on digital -safety issues.

3.1.4 Students

Students will receive an induction to Digital-Safety and correct use of college ICT facilities (hardware, network and software) during their induction to the College and will be directed to the Digital-Safety Moodle course. Issues associated with digital-safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Digital-Safety education will be provided in the following ways.

- A Digital-Safety tutorial session will be delivered to all full-time students during the induction period. Additionally this information and guidance will be made available from the portal for all students to access.
- Within classes, students 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. A range of online resources have been developed by the LRC team to further advise and guide students on staying safe online.
- A planned Digital-safety programme should be provided as part of the tutorial programme and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College.
- Students should be taught in relevant lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the student to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems and internet will be posted in all relevant rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

3.1.6

The College Digital-Safety lesson plans can be accessed on the Safeguarding portal site. Issues associated with digital-safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also 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.

This section of the policy is related to the student code of conduct and the e- safety code of conduct which is signed by all students at the beginning of the academic year.

3.2 Communication with Students

This section of the policy should be read in conjunction with the 'Staff Code of Conduct' (found on the HR Portal) and the safeguarding guidelines on the SED portal page.

3.2.1
Staff must ensure that they establish safe and responsible online behaviours. 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, web-cams, websites and blogs.

3.2.2
Staff should not share any personal information with a student. They should not request, or respond to, any personal information from the student other than that which might be appropriate as part of their professional role. Staff should ensure that all communications are transparent and open to scrutiny. Staff should also be circumspect in their communications with students so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

3.2.3
They should not give their personal contact details to students including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

3.2.4
Staff should only make contact with students for professional reasons and in accordance with College policy. Internal e-mail, One Note, Office 365 and Teams systems should only be used in accordance with the College policy. Staff should not use internet or web-based communication channels to send personal messages to students. Staff should only use equipment, e.g. mobile phones, provided by the College to communicate with students.

3.2.5
Text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible. E-mail or text communications between staff and students outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites.

3.2.6
Staff should ensure that their personal social networking sites are set at private and students are never listed as approved contacts. Staff should never use or access the social networking sites of students.

3.3 Social Networks

3.3.1
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 comment is removed and passed to the DSL/DDSL if concerns are present.

3.3.2
Social media sites can also be valuable educational resources and can, for example, be used to foster twinning relationships with overseas schools or Colleges. The College takes the view that Social media sites should not be blocked but that students should be educated about their safe use.

3.3.3
Student usage 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. It is recommended that in the classroom environment, lecturers and tutors agree behavioural rules with their groups 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 offenders.

3.3.4

Bullying or other inappropriate use of Social Media sites is a disciplinary offence for students and staff. ICT Services will assist and advise in ICT-related disciplinary investigations.

Further guidance on the use of Social Networking and Social Media is available in the 'Information Technology and Acceptable Use Policy' and the Staff Code of Practice for the Use of Social Media

3.4 Use of Images and Video

3.4.1

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.

3.4.2

All students and staff should 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. Exeter College teaching 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.

3.4.3

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 can be copied, downloaded, shared or distributed online without permission from the Head of Marketing and Communications. Photographs of activities on the college premises should be considered carefully and have the consent of Head of Marketing and Communications before being published. Approved photographs should not include names of individuals without consent.

3.4.4

Where the capture of images of students and groups have been authorised, this should be done using College media equipment only.

3.4.5

There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them. Staff need to remain sensitive to any student who appears uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings. It is not appropriate for staff to take photographs of children for their personal use. Images should be securely stored and used only by those authorised to do so.

3.5 Access to inappropriate images and internet usage

This section of the policy should be read in conjunction with the 'Staff Code of Conduct' and 'Student Code of Conduct'

3.5.1

There are no circumstances that will justify staff or students possessing indecent images of children.

3.5.2
Staff who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

3.5.3
Staff should not use equipment belonging to the College to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the member of staff to continue to work with children and young people.

3.5.4
Staff should ensure that students are not exposed to any inappropriate images or web links.

3.5.5
Where indecent images of children or other unsuitable material are found, the Police and Local Authority Designated Officer (LADO) should be immediately informed by either the Designated Safeguarding Lead (DSL) or Head of HR (or in their absence their deputies). The College should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

3.6 Personal Information and Data Protection

3.6.1
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

3.6.2
Staff must ensure that they follow the Data Protection Policy and are compliant with the Data Protection Act 2018:

- take care at all times 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;
- transfer data using encryption and secure password protected devices;
- 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 College policy (below) once it has been transferred or its use is complete.

Further detailed information is available in the Data Protection Policy 2018

3.7 Incidents and Response

3.7.1

Where a digital-safety incident is reported to the College this 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 student wishes to report an incident, they can do so to their personal tutor or a member of the Safeguarding Team.

3.7.2

Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the College 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.

3.8 Security

The college will do all that it can to make sure the college network is safe and secure. Every effort will be made to keep security software up to date. 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 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

3.9 Specific concerns

All staff should be fully aware of ongoing and emerging digital-safety concerns. Information will be passed on through safeguarding training and communicated through staff bulletins and staff development training sessions.

Tutors, through the tutorial process and other teaching staff should explore these issues as part of the wider curriculum to help equip learners to help manage their 'online life'.

These issues include but are not limited to:

- Risks around online grooming and Child Sexual Exploitation
- Risks around radicalisation and extremism
- Cyberbullying
- Viewing Pornographic material
- Viewing violent material
- Pro-anorexia/Pro-self-harm/Pro-suicide sites
- Sexting
- Gambling
- Online Fraud
- Blackmail
- Breaching Copyright laws
- Desensitisation to content
- Obsessive internet usage
- Online reputation
- Privacy and Identity Theft
- Recognising 'Fake News'

3.9 Rules for 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, in accordance with the Exeter College *Safeguarding and Child Protection Policy*:

- Permission should be sought from the individual before any image is uploaded
- 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 suitable dress should be used and group photographs are preferred in preference to individual photographs
- Parents are given the opportunity to withdraw permission for the college to publish images/audio/video of their child (if under 18) on the Exeter College website
- 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
- Content should be polite and respect others. No image should embarrass, humiliate or belittle others. Staff must be aware that images used could lead to peer on peer abuse
- Material should be proof-read (e.g. to check for spelling or grammatical errors) before being published

4 Implementation

Roles and Responsibilities

There are clear lines of responsibility for safeguarding and digital-safety within the College, anyone working with young people has a responsibility to record and report their concerns. Staff need to complete a safeguarding referral form through CPOMS where it will be dealt with by the Safeguarding Team. If their concerns relate to the conduct of a staff member then this should be passed to the Designated Safeguarding Lead (DSL) or Head of HR only (or in their absence their deputies).

All tutors are required to deliver digital-safety lessons to classes and to read through and adhere to the incident reporting procedure as contained in the Child Protection and Safeguarding Policy. When informed about a digital-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.

4.1 Staff

This section of the policy should be read in conjunction with the 'Staff Code of Conduct'

4.1.1

All staff are responsible for using the College IT systems and mobile devices in accordance with the College 'ICT Acceptable Use Policy (Staff)', which they must actively promote through embedded good practice. Staff are responsible for attending staff training on digital-safety and displaying a model example to students at all times.

4.1.2

Staff are responsible for ensuring that:

- they have an up-to-date awareness of digital-safety matters and of the digital-safety policy
- they report any suspected misuse or problem to the (D)DSL or the Safeguarding Lead for their faculty
- digital-safety issues are embedded in all aspects of the curriculum and other College activities
- students understand and follow the Digital-Safety and acceptable use policy

- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons and supported open access spaces
- they are aware of digital-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices.

4.1.3

All digital communications with students must be carried out in line with the 'Code of Practice for the acceptable use of ICT and electronic communications systems (Staff)', and the Staff Code of Conduct, and be professional in tone and content at all times. Online communication with students is restricted and must only be done through the College network or portal.

All staff should apply relevant College policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the DSL and/or the Head of Human Resources without delay (or in their absence their deputies).

All tutoring staff are required to deliver digital-safety lessons to classes as a part of the tutorial process and to read through and adhere to the incident reporting procedure.

4.2 Students

4.2.1

Students are responsible for using the college IT systems and mobile devices in accordance with the college Acceptable Use Policy and Digital-Safety Rules, which they must sign at the time of enrolment and induction. At each log-on to the College's network, all users are reminded that the following are not acceptable under the terms of this Code of Practice.

4.2.2

Students must act safely and responsibly at all times when using the internet and/or mobile technologies. This applies to all students on all college premises, in college residential accommodation and homestay accommodation, trips, visits and off site residential trips.

Students are responsible for attending digital-safety lessons as part of the curriculum and are expected to know and act in line with other relevant college policies e.g. mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe a digital-safety incident has taken place involving them or another member of the college community.

4.2.3

All students must know what to do if they have digital-safety concerns and who to talk to. In most cases, this will be either speaking with a member of staff or submitting a Safeguarding Report Form on the Student Experience Portal. Where any report of a digital-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. All digital-safety issues will be treated seriously and additional support provided by tutors or the Safeguarding/Welfare Team. Where appropriate students may be signposted to external agencies for additional support.

4.2.4

Students are responsible for ensuring:

- that they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- the need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- they know and understand College policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying
- they understand the importance of adopting good digital--safety practice when using digital technologies out-of- College and realise that the College's Digital-Safety policy covers their actions out of College, if related to their membership of the College.

4.3 Digital-Safety Lead on the Safeguarding Group

The Digital-Safety Lead is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to lead on digital-safety as part of the cross college Safeguarding group, contribute to any review and updates to the Digital-Safety Policy, deliver staff development and training where requested and support the investigation of digital- safety incidents if required by the DSL/DDSL and Safeguarding Team.

4.4 Governors

Governors are responsible for the approval of the Digital-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors / Governors Sub Committee*. There is a nominated Governor for Safeguarding , which incorporates digital -safety. The Governor with responsibility for safeguarding will :

- meet regularly with the DSL;
- report to the Governing Body on Safeguarding; including digital safety

4.5 Monitoring extremist content

The DSL and DDSL will receive weekly reports compiled by IT Services (filtered by Fortinet software) 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.

5 Associated Documentation

This Digital-Safety policy should be read in conjunction with the following College policies:

- Child Protection and Safeguarding Policy and Procedures
- Code of Practice on the use of Social Media (Staff)
- Data Protection Policy
- Digital Learning Plan
- Electronic Communications CoP Staff
- Electronic Communications CoP Students
- ICT Acceptable Use Policy
- Information Security Policy
- Staff code of conduct
- Student Code of Conduct including the acceptable use of IT agreement.
- Tutorial Policy

6 Monitoring, Review and Evaluation

This policy has been created collaboratively by the College Safeguarding Team which comprises:

- Designated Safeguarding Lead
- Deputy Designated Safeguarding Lead
- Safeguarding Team
- Assistant Principal with responsibility for Safeguarding
- Designated Safeguarding Governor
- Head of Human Resources
- Head of Estates
- ILS Customer Experience Manager

Consultation was carried out with a selection of staff and students.

The impact of the policy will be monitored regularly with a full review being carried out every 2 years or more regularly in the light of any significant new developments in the use of the technologies, new threats to digital-safety or incidents that have taken place. The policy will also be reconsidered where particular concerns are raised or where a digital-safety incident has been recorded.

7 Equality Analysis

Please use the 'equality analysis procedure' to guide you to complete the text boxes below, expanding them as you wish. If this is a review and you have made changes - please add date and make any amendments if required.

September 2018

7.1. Is your policy equality- relevant? If yes, please list which groups of people will be affected by this policy.
All students and staff.

7.2. How have you involved people from minority groups who may be affected by this policy?
Describe any activities such as conversations, interviews, feedback or plans to do this in the future. The policy applies to all groups.

Staff – questionnaire (annual)
Student (SPQ)
Learner Voice feedback

7.3. What evidence have you considered?

The South West Grid for Learning.
The Department for Education.
The general principles outlined in the 'Working together to safeguard children (2018) HM Govt.
Keeping Children Safe in Education – information for all school and college staff Dfe September 2018.

Safeguarding Cross College Team
Government Lead Child Sexual Exploitation Data

7.4. How will your policy fulfil the public sector duty by helping fight discrimination, advance equality of opportunity and foster good relations?

Characteristic	How does your policy help fulfil the public sector duty?
Age	*This policy applies equally to all protected characteristics. Consultation was carried out with a selection of staff and students. The impact of the policy will be monitored each term by the Safeguarding team and fully reviewed every 2 years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to* digital-*safety or incidents that have taken place.*
Disability	
Sex	
Pregnancy & Maternity	
Marriage and Civil Partnership	
Race	
Religion and belief	
Sexual Orientation	
Gender Reassignment	

7.5. Describe any potential adverse impacts that may arise as a result of the policy. None