Date: September 2023
Author: Deputy Head Pastoral
Owner: Deputy Head Pastoral

Document No: SPS_ICT_001
Version: 001

E-Safety and Safe Use of Technology Policy

2023-2024

The policy is applicable to all students, staff, governors, and visitors.

Legal Status

This policy has been prepared with reference to:

- The Equality act 2010
- Early Years Foundation Stage 2017
- Prevent Strategy 2015 updated 2019
- Data Protection Act 2018

Related Documents

This policy should be read in conjunction with:

- SEND policy
- Staff Code of Conduct
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- EYFS Policy
- GDPR & Data Protection Policy
- Device User Agreement
- Safeguarding Policy

Aims

We are committed to providing a caring, friendly, and safe environment for all our students so that they can learn in a secure atmosphere. This extends to the virtual environment. We are committed to safeguarding the well-being of our students whether they are on-line or using other multimedia technologies. We are also committed to supporting parents and the community in understanding how the use of technology at home can affect life at school.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing a significant role in the everyday lives of children, young people, and adults. Consequently, schools need to build in the use of these technologies to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society. Currently the internet technologies staff, children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging, and Teams
- Social Media, including Facebook and Twitter (For marketing purposes by staff members only)
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Sherborne Prep**,** we understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Sherborne Prep holds personal data on learners, staff, and other people to help them conduct their day-today activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Monitoring

ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving the school's students, without consent, to the extent permitted by law. This may be to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a student may result in the temporary or permanent withdrawal of school ICT hardware, software, or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the school's procedures.
Breaches may also lead to criminal or civil proceedings.
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's DSL, and IT Manager. Additionally, all security breaches, lost/stolen equipment, or data (including remote access login information and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non- compliance must be reported to the school's DSL and IT Manager.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, are automatically checked for any viruses using school provided antivirus software before being used (Removable media is automatically scanned when connected to a school computer)
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your school device is not routinely connected to the internet, you must make provision for regular virus updates through the IT Department

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the IT Support Department immediately. The IT Support Department will advise you on what actions to take and be responsible for advising others that need to know.

Digital Communication (Email and Chat)
The use of electronic communication within most schools is an essential means of communication for both staff and students. In the context of school, e-mail and chat should not be considered private.
Educationally, e-mail and chat feeds can offer significant benefits including direct written contact between schools on different projects, be they staff based or student based, within school or externally. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette.'

Managing Digital Communication

- All students have their own individual school issued accounts.
- The forwarding of chain letters is not permitted in school. However, the school has set up an account (helpdesk@sherborne.org) to allow students to forward any chain letters or any other content causing them anxiety. No action will be taken with this account by any member of the school community other than the IT Support Department.
- All student digital communication users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in digital communication or arrange to meet anyone without specific permission.
- Students must immediately tell a teacher\ trusted adult if they receive an offensive e-mail or message.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Students are introduced to e-mail and Teams Chat as part of the ICT Scheme of Work.

Equal Opportunities

Students with Additional Needs:
The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the school's E-Safety rules.

However, staff are aware that some students may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E- Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum, and we continually look for new opportunities to promote E-Safety. We are also committed to providing support and guidance to parents and carers in how to manage e-safety and use of technology at home.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Students are taught about copyright, respecting other people's information, safe use of images and other key areas through discussion, modelling and appropriate activities.
- Students are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e., parent \ carer,

teacher \ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button, link below.

https://www.ceop.police.uk/ceop-reporting/

- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Managing the School E-Safety Messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The E-Safety policy is introduced to new students at the start of each school year with key aspects highlighted annually to all students
- Students starting at Sherborne Prep mid-year will undergo catch-up sessions
- E-Safety posters will be prominently displayed
- The key E-Safety advice will be promoted widely through school displays, newsletters, and curriculum activities

Managing the Internet

The internet is an open worldwide communication medium, available to everyone always. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people.
All use of the **School Internet Service** is logged, and the logs are randomly but regularly monitored.
Whenever any inappropriate use is detected, it will be followed up.

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and wireless internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with students.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must always observe software copyright. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Technology Use

- You must not post personal, sensitive, confidential, or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- You must not reveal names of colleagues, students, others, or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed. (There are some controlled exceptions for gaming in the boarding wing and during ICT Lessons).

Staff and students are aware that school-based email and internet activity can be monitored and explored further if required. (This is repeated in the first bullet point below)

In common with other media such as magazines, books and videos, some material available via the internet is unsuitable for students. The school will take all precautions to ensure that users can only access appropriate material. However, due to the international and linked nature of internet content, it is not possible to guarantee that unsuitable material will never occur on a school computer. The school cannot accept liability for material accessed, or any consequences of internet access.

Infrastructure

- Sherborne Prep has an internal monitoring solution powered by an Opendium Firewall appliance where web-based activity is monitored and recorded.
- School internet access is controlled through the Opendium web filtering service.
- Staff and students are aware that school-based email and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off\ closed and the incident reported immediately to the DSL, teacher, or IT Support Department as appropriate.
- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the IT Department's to install or maintain virus protection on personal systems. (If students wish to bring in work on removable media it must be given to the Teacher or the IT Support Department for a safety check first, when possible, although school pcs will automatically scan any device plugged in.)
- Students and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Digital Lead, Subject leader, or the IT Department.
- Wherever possible students using personal electronic storage devices must make sure they have a backup copy of any data on their school account. Sherborne Prep is not responsible for any data or coursework\Controlled Assessment lost due to the failure of a personal electronic storage device.

Managing Other Web Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative, and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture, and commercialism. To this end, we encourage and educate our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to students within school (With some controlled exceptions for boarders and ICT lessons). Day children are not permitted to have a phone in school, however, if a phone does come to school, it must be handed to the office or, if boarding, locked in the boarders' common room.
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites or social platforms and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile\home phone numbers, school details, IM\ email address, specific hobbies\interests).
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our students are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis, or other online areas in order to communicate with students using the school Office 365 tools or other systems such as Microsoft Teams approved by the Head.

Parental Involvement

We believe that it is essential for parents\carers to be fully involved with promoting E-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E- Safety with parents\ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

- Parents\carers must read through and sign the acceptable use agreements on behalf of their child on admission to the school.
- Parents\carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents\carers must sign the E-Safety agreement on joining the school containing the following statement:
- "We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community"
- The school disseminates information to parents relating to E-Safety where appropriate in the form of:
    - Information evenings
    - Practical training sessions e.g. How to adjust social media privacy settings
    - Posters
    - School website and newsletter items
    - Parents are made aware that there is a Communications Policy in place that sets guidelines on hours that staff should be contactable, this is held on the parent portal

Parents are also made aware of the guidelines in the boarding house as a framework for device usage at home- specifically relating to screen time.

Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to authorised IT staff when necessary, and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Passwords must contain a minimum of eight characters and be difficult to guess.

- Passwords should contain a mixture of upper and lowercase letters, numbers, and symbols.
- User ID and passwords for staff and students who have left the school are disabled from the system within 24 hours.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers, or other students.

If you think your password may have been compromised or someone else has become aware of your password report this to the IT department.

Publishing Students' Images and Work

On a child's entry to the school, unless consent is withdrawn by parents on receipt of letter to the Head (on behalf of students) and staff, student images and work may be used in the following ways:

- On the school web site.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- On the school's social media streams.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e., exhibition promoting the school.
- General media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g., divorce of parents, custody issues, etc.

- Parents, carers, or students may withdraw permission, in writing, at any time.
- Students' full names will not be published alongside their image and vice versa. Email and postal addresses of students will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
- Only the designated staff member for the relevant Web section has authority to upload to the site.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, Tablets, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Mobile devices that can access the internet via a mobile phone network generally provide unfiltered web access. Such devices are not permitted for use by students during the school day. The school day includes any time spent on a school bus.

Boarders are permitted to have smart phones but may only access these out of school hours with permission and within a set period. All devices must be stored in the designated areas within the boarding

house. Devices may be checked sporadically by boarding staff at the beginning of term and throughout the academic year for unsuitable content.

It must be understood that, whilst in school, all devices are subject to the same rules as school computers whether accessing the internet through the school's Wi-Fi network or through mobile broadband. Mobile devices are also filtered through the school's filtering system if connected to the network and therefore, the same acceptable use policy will apply. All devices will use the schools Wi-Fi unless express permission has been given by a member of staff.

BYOD (Bring your own device)

Sherborne Preparatory School provides a modern technology-based learning environment for students. We have a fully equipped ICT classroom with 20 desktop, touch-screen computers. The school also provides one-to-one laptops to every student in Years 7 & 8; banks of iPads are available for classroom use from Reception to Year 6.

It may be appropriate, at times, for a student in Years 5 of 6 to bring in their own digital device to aid them in the learning that takes place within the classroom.

The School is not liable in any way for any device brought into school and accepts no responsibility for the damage, loss, or condition of any student-owned device. It is the responsibility of the parents to take out adequate insurance to cover such potential damage or loss.

The school does not allow student mobile phones of any kind on School premises (Except in the boarding house, where appropriate rules apply.) and this Bring Your Own Device Policy does not consider mobile phones as a suitable digital learning tool. Smart Watches are considered part of this Policy, although any device that has a cellular capability (i.e. using mobile broadband) will not be allowed to be used in school.

The following rules are to be used in line with the E-Safety & Use of Technology Policy (This document), Behaviour Policy, Data Protection Policy as well as other School policies, where applicable.

Failure to follow the rules stated will result in a student having the privilege of bringing in their own device taken away.

All student-owned (and the ones we provide for them) devices that are connected to the Sherborne Prep network must follow the following regulations:

- All access to the internet at School on any device must be via the school-provided Student Wi-Fi and not via 3G/4G/5G or other mobile data.
- All devices must have password, PIN, pattern, or fingerprint security access in place and users must never share this information with other students.
- Students may not use or interfere with another student's device without explicit permission.
- Student-owned devices must not be used to make audio or video recordings or to take photographic images during the school day or on School premises, unless explicit permission is given by a member of staff, as well as by any student being recorded.
- Any images, videos or audio recordings must be deleted from the student's device before the end of the lesson. If needing to be saved, these must be uploaded to the student's cloud-based storage area within that lesson period.
- Student-owned devices should not be used when walking around the school site, nor headphones worn at any time other than when directed by a member of staff during a lesson.

- Students are reminded to securely store their device, when not in use, within their own locker and that the device has a suitable case

- Students are reminded of the importance of bringing their device to School each day fully charged. The school has very limited charging facilities for students' own devices.
- All devices should only be used within a lesson context and not during break times or unrelated lessons. Student-owned devices should not be used in School to access any form of social media.
- Playing online games student during the school day is not permitted, unless a teacher has given permission
- Parents and students are responsible for ensuring that no inappropriate apps, material, images, or videos are on their devices.
- Students are reminded that the use of a digital device is intended to support their learning experience and any device used in a lesson must only be used as directed by the teacher in charge of the class.
- Digital devices must never be taken into any of the school changing rooms.
- Using internet-, device- or app-based messaging in class is not allowed except the class chat in Microsoft Teams.
- Using a device connected to a cellular network (i.e., mobile broadband) to make telephone calls is not allowed.
- Students should only store/archive their schoolwork in their Microsoft 365 account provided by the school.
- The school reserves the right to examine any device brought into school which has connected, or could be connected, to the school network.
- Anti-virus software must be installed on devices where applicable.
- The school provides Microsoft Office 365 to all students and will support students in setting this up on a device.
- Students may be required by the school to access the App Store, Google Play, or other similar app stores to download free apps at times.
- Students will have the ability to print from their own device using the School's Papercut service. This is always to be used with consideration for the environment.
- Attempting to circumnavigate the School's IT security systems is prohibited.

To conform to Health and Safety compliance, any defective or damaged devices should not be brought into the school. Parents are responsible for checking for any issues before a device is brought in.

The school actively monitors internet searches in School and, as a student's own digital device will be connected to the school Wi-Fi, we may store and collect search data for each user and store this within our secure network.

Any third-party apps we use in School are carefully selected and students are taught about the importance of keeping their personal data safe as part of the school's e-safety curriculum.

Home and School E-Safety Agreement

This agreement is designed to ensure that we are all working together to help the students stay safe and learn how to use and navigate the online world. Both the student and the parents/carer need to sign this agreement having looked through it together.

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own username and password.
- I will follow the school's ICT security system and not reveal my passwords to other students and change them when requested by the ICT Teacher.
- I will only use my school e-mail address for school related purposes.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored, and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Head.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students, or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will always respect the privacy and ownership of others' work on-line.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and that this will be seen by the Deputy Head Pastoral.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent /carer may be contacted.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents /carers recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- Parents/carers understand that if they permit their child to use mobile technology that they will monitor usage.
- The school strongly suggests that parents/carers follow the rules that the school boarding community follow:

1. Children do not use mobile technology after 8pm.

2. Mobile technology is only permitted in communal areas, although boarders are given quiet spaces to talk to family.
3. Mobile phones are never permitted in bedrooms.

Please note the current age restrictions for some of the main social media apps.

	Instagram: Minimum age to have an account is currently 13 years old.
	Facebook: Minimum age to have an account is currently 13 years old.
	X (previously known as Twitter): Minimum age to have an account is currently 13 years old.
	Snapchat: Minimum age to have an account is currently 13 years old.
TikTok	TikTok: Minimum age to have an account is currently 13 years old.

E-Safety

Dear Parents \ Carer

ICT including the internet, e-mail, mobile technologies, and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of E-Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss the agreement attached with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the school Digital Lead.

Please return the bottom section of this form to school for filing.

✂

Student and Parent \ carer signature

We have discussed this document with …….. (Student name) and we agree to follow the E-Safety rules and to support the safe and responsible use of ICT at Sherborne Prep.

Parent\ Carer

Signature…….

Date ……

Student

Signature…….

Form ……

Date ……