Internet and Acceptable Use Policy

Written by	Director of IT Systems, Data and Compliance
Date for Review	September 2019
Authority	Headmaster
ISI Policy Code NMS	

Sherborne Preparatory School aims to ensure secure access to the internet and technology for all pupils, staff and visitors. This policy outlines the acceptable use of internet and electronic mail facilities, file-servers, messaging services and any networks or hardware, including but not limited to that provided by the school. It applies to any personal devices and other equipment that can be used to access, store or record data or media files.

Why do we use the internet in school?

Digital technologies have become integral to the lives of children and young people in today's society. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone.

The purpose of internet use in school is to support teaching and learning and with-it pupil achievement. It is also supports the daily business and administration of the school.

Sherborne Preparatory School believes that pupils, staff and visitors have a right to safer internet access at all times. As a school, we believe that the possible benefits of using the internet outweigh the possible risks.

The curriculum requires pupils to learn how to use computers in a responsible, effective and safe manner in a way that supports their learning within the school community. It also requires pupils to learn how to locate, retrieve and exchange information using technology.

Effective Internet use is an essential life-skill for all pupils to master and the pupils take part in a lesson on E-safety at least once a term.

The school keeps a record of network users within the school's servers and carefully sets access rights to ensure pupils, staff and visitors are able to access the online-shared areas as needed while maintaining levels of security.

In common with other media such as magazines, books and videos, some material available via the internet is unsuitable for pupils. 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.

If pupils discover unsuitable sites, the URL (address) and content should be reported immediately to the Director of IT Systems, Data and Compliance or another member of staff.

Each pupil, from the Year 3 upwards, will have his or her own login and password to gain access to the school's network.

Pupils must not reveal details of themselves or others, such as their address or telephone number, or arrange to meet anyone in e-mail communication. Pupils must immediately tell a member of staff if they receive any offensive messages.

Pupils will be made aware that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Pupils will also be educated in how to remain safe when using the internet. Pupils use of the internet will be monitored for content and possible attempts to access barred content. Emails may be monitored at any time, as deemed fit. This is to safeguard pupils.

This acceptable use policy is to be used in line with other school policies.

Core Principles

To ensure responsible use and the safety of pupils, the school's policy is built on the following core principles:

Responsibility

Internet safety depends on pupils, staff, parents and all members of the school community taking responsibility for their use of the internet and the use of technology.

We recognise that internet safety is a child protection and general safeguarding issue. Staff are made aware of the safety issues involved with the misuse of the internet and digital devices. As a school, we work with the Local Safeguarding Children's Board (LSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of Sherborne Preparatory school.

The school's digital safety is the Director of IT Systems, Data and Compliance's responsibility. As a school, we ensure that staff and all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. Any allegation of misuse on the internet or using a digital device shall be handled by the Director of IT with the involvement of other staff members depending on the circumstances.

Education

All pupils in Year 1 through to year 8 will discuss and learn about acceptable uses of the internet and its possible dangers as part of the IT and Computing curriculum. These topics may also be covered as part of the Personal Development lessons and during form time where appropriate. Pupils will know what to do if they come across inappropriate material when using the internet.

We seek to work closely with parents and guardians in promoting a culture of digital safety. We will contact them if we have any worries about their son or daughter's behaviour in this area, and we hope that they will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use digital devices at home. We therefore, arrange information workshops for parents where advice is made available, concerning the potential hazards of using technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

Technical Prevention

The school invests in technical solutions (Internet filters and firewalls) that aim to prevent access to unsuitable material on the internet, although it is accepted that no technical method can be 100% effective. All internet traffic is monitored regularly, and any user found to be accessing inappropriate sites will be offered support and guidance. A daily report is sent to safeguarding team that included staff responsible for overseeing various aspects. Repeat offences will be logged on iSams.

Mobile devices and Smart Phones.

Mobile devices that can access the internet via the 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 and tablets but may only access these out of school hours with permission. All devices need to be stored in the designated areas within the boarding house. Devices may be checked sporadically by the Housemaster and mistress 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 as outlined below will apply.

ACCEPTABLE USE POLICY

Sherborne Preparatory School has a range of technology located around the school site. All of these resources are designed to support teaching, learning, and the administration of the school.

The acceptable use policy will be prominently displayed as a constant reminder of the expectations regarding internet use. These rules are set out below, along with sanctions that may be applied if the rules are not followed:

Network security

- ✓ I will only access the computer system with the login and password I have been given.

- ✓ I will not give out my password to anyone else. If I suspect that my password has been discovered I will report this to the Director of IT and have it changed immediately.
- ✓ I will not download, install, modify or remove programs on the school's computers.
- ✓ I will not modify the computer's hardware in any way.
- ✓ I will not leave an iMac, PC, laptop or tablet logged on and unattended.
- ✓ I will not use the school computer network to attempt to gain access to unauthorised computer networks or any other "hacking" activity.
- ✓ I will not try to bypass the school's filtering system.

Email

- ✓ I will not use the computer facilities to threaten, harass or upset others.
- ✓ I will only use my school email for school related activity.
- ✓ I understand that my emails should be polite and considerate. I will refrain from using offensive or explicit language in my e-mails and will encourage persons who contact me to do the same.
- ✓ I will carefully consider the content of attachments on outgoing email and not send intolerant material in any form.
- ✓ I understand I will need to check my school email regularly.

Data

- ✓ The school reserves the right to share personal details of users with third parties should this be needed when investigating conduct online which has an impact on school life.

Resources

- ✓ I will only use my personal server folder to store school work unless permission is given to save it within a local shared area.
- ✓ I understand I am allowed to use OneDrive and other cloud-based applications to store school related files.
- ✓ I understand that I must ask permission before using USB devices in school.
- ✓ I will not deliberately waste valuable resources including paper, printer toner and disk space.

The law

- ✓ I will obey all laws, including those that prohibit unauthorised copying of software, music and films.
- ✓ I understand and agree that my computer files and the contents of my mailbox can be checked and that the internet sites that I visit may be monitored.

Internet

- ✓ I understand that I will only use the internet for school work.
- ✓ I will not access any Internet chat rooms or social networking websites.
- ✓ I will report any questionable material to a member of staff immediately.
- ✓ I will not use any form of electronic communication in any way that may prove harmful to the school, its staff or pupils.

- ✓ I understand that I am strictly forbidden from using any form of internet file-sharing software
- ✓ I will not tag or name pupils, staff or any other aspect of the school in photographs or posts online, either during school time or during the holidays.
- ✓ I will not engage in any online activity that brings the school into disrepute.
- ✓ I will not try to follow or befriend any member of staff past or present on social networking sites.

Sanctions

- ✓ Violations of the above rules will result in a temporary or permanent ban on internet use.
- ✓ Additional disciplinary action may be added at the discretion of the Director of IT Systems, Data and Compliance or the Headmaster.
- ✓ When applicable, police or local authorities may have to be involved.
- ✓ A log will be kept of all breaches of this policy in the pupil's digital school file on iSams.

By accessing and logging into the Sherborne Preparatory School network users automatically agree to follow the above acceptable use policy.

Staff members also sign a document to show that they have read and understood the details outlined in this policy.

Charter for the safe use of the internet and electronic devices

Digital safety is a whole school responsibility, and at Sherborne Preparatory School, the staff and pupils have adopted the following charter for the safe use of the internet inside the school. We also expect parents to support the school in this by putting in place clear digital safeguards for their son or daughter at home in line with school expectations.

Cyberbullying

- ✓ Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- ✓ Proper supervision of pupils plays an important part in creating a safe IT environment at school; but everyone needs to learn how to stay safe outside of school.
- ✓ Cyberbullying and or harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating Other Users with Respect

- ✓ We expect all members of the school community to treat each other online with the same standards of consideration and good manners as they would in the course of face to face contact. They should always follow the school's Rules and Regulations.
- ✓ We expect a degree of formality in communications between staff and pupils, and would not expect them to communicate with each other using any form of digital communication other than that provided by the school.
- ✓ Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-bullying policy is set out in the School Handbook. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- ✓ All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issues to a member of staff.

Keeping the School Network Safe

- ✓ We agree to follow the Acceptable Usage Policy.
- ✓ We adhere to best practice regarding use of the internet.
- ✓ Certain sites are blocked by our filtering system and the Director of IT Systems, Data and Compliance monitors pupils' use of the network.
- ✓ We issue pupils in Year 5 to 8 with a school email address. Access is via a cloud portal, which is password protected.
- ✓ Users are also provided with Google accounts which allows them to access documents and the school's VLE.
- ✓ We give guidance on the reasons for always logging off and for keeping all passwords secure.
- ✓ Access to other external email providers are not allowed on the school's network by students but staff may use these if needed.
- ✓ We have anti-virus protection on our network.
- ✓ Any member of staff or pupil, who wishes to connect a removable device to the school's network, is asked to arrange in advance with the Director of IT Systems, Data and Compliance to check it for viruses.

Promoting Safe Use of Technology

We expect parents to monitor their children's access to social media and video games and to follow the age restrictions put in place by these providers.

Staff, pupils and parents are encouraged to make use of the excellent online resources that are available from sites such as:

- ✓ UK Council for Child Internet Safety (www.dcsf.gov.uk/ukccis)
- ✓ Think you Know (www.thinkyouknow.net)
- ✓ Childnet International (www.childnet-int.org)
- ✓ Digizen (www.digizen.org.uk)
- ✓ Cyber Mentors (www.cybermentors.org.uk)
- ✓ Cyberbullying (www.cyberbullying.org)
- ✓ E-Victims (www.e-victims.org)
- ✓ Bullying UK (www.bullying.co.uk)

They prepare their own models of good practice, which form the subject of lessons, discussions and presentations during assemblies.

They cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving yourself from future embarrassment, explaining that any comment or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, server or internet archive and cause embarrassment years later.

The Director of IT Systems, Data and Compliance has an open door policy and is available to support pupils, staff and parents should further guidance and support be needed.

Safe Use of Personal Electronic Equipment

- ✓ We offer guidance on the safe use of social networking sites and cyberbullying during computing lessons, which covers blocking and removing contacts from "friend lists".
- ✓ Lessons include guidance on how pupils can identify the signs of a Cyber- stalker, and what they should do if they are worried about being harassed or stalked online.
- ✓ We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the digital world.
- ✓ We give guidance on how to keep safe at home, by encrypting your home wireless network, not opening unknown attachments and reporting any illegal content.
- ✓ We advise on the responsible use of skype and FaceTime.

Considerate Use of Electronic Equipment

- ✓ Use of mobile phones during the working day is forbidden for all pupils.
- ✓ The use of cameras on mobile phones by pupils is not allowed on the school premises or during any school excursions.
- ✓ Staff may bring mobile phones to school, but they should use their professional discretion as to when to use these and in line with other school policies.
- ✓ Staff should not take pictures of pupils only in line with the school photography and recording policy.
- ✓ Staff may confiscate personal equipment that is being used during the school day for periods of up to 7 days.
- ✓ Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

We expect all staff, pupils, parents, visitors and members of the school community to adhere to this charter for the safe use of the internet.