Acceptable Use Policy (for Staff & Volunteers)

Rationale

This policy covers responsible use of mobile devices, internet/networks, emails and personal devices in school. Chapmanslade School recognises the important contribution and value technology can play in promoting students' learning and development, however, there are potential risks involved. We have rigorous online safety policy and procedures in place and have taken positive steps to reduce this risk in school, as we believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed the disadvantages.

Allowing the use of internet and mobile devices is a school decision, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment;
- Users have access to resources to support learning and teaching;
- Users should be given clear boundaries on responsible and professional use.

Use of Technology

Access to network services is given to users who act in a considerate, appropriate and responsible manner. Users are responsible for their behaviour on school networks just as they are in any part of the school. Access is a privilege, not a right, and entails responsibility. We expect all users to use technology, both that belonging to the school or their own, responsibly and strictly according to the following conditions:

(For the purposes of this document, technology means any device that provides a connection to the Internet or internal network or take photographs.)

1. A device loaned to you by the school for an education related purpose remains the property of Chapmanslade School;
2. Only approved user devices may connect to the school network by prior agreement;
3. Personal devices must remain in your possession, and should be securely stored when not in use (with the exception of smart watches – see personal devices heading below);
4. This policy regarding the appropriate use and sharing information applies to devices both school and privately owned. Use of any device must adhere to data protection; online safety and health and safety rules;
5. Devices may be used for education related purposes at the discretion and under the supervision of the teacher.
6. If used to create or store personal information including images and videos of pupils, users must fully comply with high standards of data protection as set out in the Data Protection Act 1998.

7. A device connecting to the school network may be configured with certain restrictions in place. Any settings that are passcode protected must not be changed.

8. Insurance cover provides protection for school owned devices from the standard risks whilst the device is on site or in your home but excludes theft from a car or other establishment. Should the device be left unattended and is stolen, you will be responsible for its replacement.

9. Privately owned devices remain the responsibility of the owner and will not be covered under the school insurance policy.

10. All devices, whether owned by the school or privately owned, may be subject to regular checks for compliance with school policies. Failure to comply or evidence of unacceptable use will result in sanctions or disciplinary action.

Unacceptable use includes but is not limited to:

- Make, store, post, download, upload or pass on, material, remarks or images that may be offensive or upsetting to an individual or group;
- Make, store, post, download, upload or pass on images of individuals without their permission (or in the case of images of pupils, the permission of their parent or carer);
- Giving personal information, such as complete name, phone number, address or identifiable photo, without permission from teacher and parent or guardian;
- Using obscene language;
- Damaging or modifying computers, computer systems or computer networks: downloading, installing and using games, audio files, video files or other applications including shareware or freeware without permission to do so;
- Sharing or using others' log on details, passwords or other confidential information;
- Trespassing in others' folders, work or files;
- Intentionally wasting limited resources;
- Employing the network for non-academic, personal, commercial, political purposes, financial gain, or fraud;
- Attaching unauthorized equipment to the school network;
- Updating web pages etc. or use pictures or text that can identify the school;
- Attempting to repair or interfere with the components, software or peripherals of any computer that is the property of Chapmanslade School.

You are reminded that you are always subjected to the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and General Data Protection Regulations 2018.

Mobile Devices (e.g. laptops, iPads, Cameras, Smart Watches)

1. The device remains the property of Chapmanslade School.

2. The device is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated.

3. All teacher devices must be password protected. A universal 'Chapmanslade password' will be used for locking iPads.
4. On the teacher leaving the school's employment, the device is to be returned to Chapmanslade School on the day of leaving unless otherwise agreed with the headteacher. Staff on extended leave of 4 weeks and over (e.g. maternity leave) should return their device to the school (other than by prior agreement with the headteacher).
5. When in school and not being used, the device must be locked. All laptops should be shut down at the end of the school day.
6. If the device is taken out of school it should not be left in an unattended car. If there is a need to do so it should be locked in the boot.
7. The device must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
8. Staff should not load their own software onto the laptop unless agreed with senior leaders (it must be fully licensed and not corrupt any software or systems already installed on the device).
9. Any software loaded must not affect the integrity of the school network.
10. Removable media (such as USB memory sticks), other than that which has been authorised by Chapmanslade School must not be used.
11. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
12. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
13. Pupils may only use a PC or staff laptop if logged in as themselves. Teachers must not log on for students.
14. Users are responsible for charging their own devices and for protecting and looking after their devices while in school
15. If any fault occurs with the device, it should be referred immediately to our managed service provider, Agile ICT.
16. The device would be covered by normal household insurance. If not, it should be kept in school.
17. All teacher laptops should not have any sensitive data saved on them, particularly on the computer's desktop area. All sensitive data should be saved in the designated place on the school server or within the teacher's Microsoft OneDrive. This can then be accessed via a remote connection when off-site.
18. Should a school device be lost, the headteacher must be notified immediately.

E-mail, Network and Internet use

- School provided services must only be accessed with an individual's own name and registered password, which will be kept secret.
- The headteacher should be informed immediately if passwords are no longer secure.

- Services should be logged off of when work is finished.
- The school may, in line with policy, check computer files and e-mails and may monitor the Internet sites visited by individuals.
- If these rules are not adhered to, network access will be suspended immediately, devices will be taken and that other disciplinary consequences may follow.

E-mail

School teaching/admin staff and governors have all been provided with an Office 365 account.

1. E-mail attachments are only to be opened if they come from a recognised and reputable source. Any other attachments will be brought to the attention of the senior leadership team.
2. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
3. It is the account holder's responsibility to manage their own e-mail inbox. In line with GDPR 2018 regulations, emails should be regularly sorted and unnecessary emails deleted. Emails over a year old should only be kept if truly necessary.
4. Unpleasant material or messages must be reported immediately to the headteacher.
5. Any confidential e-mails must contain 'CONFIDENTIAL:' within the subject.

School Server and Network

School teaching/admin staff and governors have access to the school network and server both within school and at home.

1. 1 Files should be stored in the appropriate drive locations as listed below (users will only see drives relevant to them)
2. When accessing the server from home, this must not be left unattended. Users must log off immediately when finished.

Internet and Online Services

The school internet is filtered by SWGfL (South West Grid for Learning). Members of staff have different rights to that of pupils, allowing them to access more content. The school uses online services for teaching and learning (e.g. Mathletics).

1. It is criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
2. Any e-safety concerns should be raised with the senior leadership immediately.
3. Should any inappropriate material appear, please report this to the computing leader immediately, who will follow the SWGfL Online Safety Incident Flowchart (see Appendix 2).
4. No data or personal information is to be stored on online services unless subscribed to by the school. First names and initials should be used only if possible.

Personal Devices

1. Pupils must not bring in personal devices for use in school (Should this happen, the device should be looked after by class teacher in their desk drawer until the end of the school day).
2. Pupils must not bring in watches which include cameras.

3. Any external USB devices are not to be used in school. Only school approved USB devices should be used. These should ideally be encrypted.
4. Members of staff should not use any personal devices in school other than mobile phones, which must only be used in child-free areas (the staff room, headteacher's office and main school office) during school hours.
5. Photographs of children must never be taken on any personal device.
6. Mobile phones must not be connected to the school's Wi-Fi network.
7. If connecting to the internet via cellular (3G/4G/5G) in school, acceptable use still applies. Individuals must not access any inappropriate content.
8. If school email accounts are accessible on a personal device, these must be password or fingerprint protected. No files should be downloaded onto the personal device.
9. All staff and volunteers must read and sign Use of mobile phones in school document (Appendix 1).

Review

This policy should be publicised to staff, parents and pupils at least once a year. It will be reviewed no later than every two years.

Updated 15th September 2022

Reviewed: August 2023

Next Review: August 2025

Appendix 1: Mobile phone use in school

Dear Staff, Parents and Visitors,

Re: Use of Mobile Technologies on School Premises

Our policy on use of mobile technologies exists to safeguard the welfare of children in our school.

Mobile phones may be brought into school. While working or visiting the school, phones should always be out of sight, turned off/silent. Under no circumstances (including on school trips) may mobiles phones be used to take pictures or makes sound or video recordings of children. Mobile phones are only to be used in the Staff Room, Headteacher's Office or Main Reception Office during the school day.

A copy of our acceptable use policy is available to view on the school website or a paper copy is available from the office on request.

I should be grateful if you could complete the slip below and return it to the office.

Yours sincerely,

Robert Cottrell

Chapmanslade School
Headteacher

USE OF MOBILE PHONES IN SCHOOL

I agree to abide by the school's acceptable use policy and only use my mobile phone in the designated areas.

Name: …….. Signed: …… Date: …….

Appendix 2: SWGfL Online Safety Incident Flowchart