



Chipping Sodbury School

Online safety procedure

Updated	March 2025
Review date	March 2027
Linked policies	Anti-Bullying Procedure Staff Code of Conduct Athelstan Trust Behaviour Policy Child Protection and Safeguarding Policy Inclusion Policy

Rationale

New technologies are 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. Electronic communication helps teachers, students and parents learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. However, new technologies can put young people and the adults who work with them at risk within and outside of school, and it is with a view to safeguarding that this policy is created.

Aims

- To provide a framework for students and staff to recognise and avoid risk, and for remaining safe when using messaging services, social media and the internet
- To demonstrate our commitment to safeguarding our school community

Guidelines

- A planned and up-to-date online safety programme will be provided as part of ICT and Life curriculums, covering both the use of ICT and new technologies inside and outside of school
- Acceptable use agreements will be signed by students and parents/carers yearly and a display on log-in screens will remind users of their responsibilities
- Staff acceptable use agreements will be signed on receipt of their staff laptops
- Key online safety messages will be reinforced in safeguarding assemblies and through curriculum content including safe use of the internet and protecting passwords
- Students will be taught explicitly to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information from three independent sources
- Students will be taught to acknowledge the source of information and to respect copyright
- In lessons where internet use is pre-planned, students will be guided to sites checked for suitability by staff and IT Support will be informed if any unsuitable materials are found. Impero or close monitoring by staff will occur when "free" searches of the internet are suggested. Impero can be used to allow only specific sites and can block internet use completely

Responsibilities have been identified for different members of the school community and as such these will be at different levels depending on the position of the individual or group within the school. Our core responsibilities to online safety are:

Governing Body

- Approving the Online Safety procedure and reviewing its effective implementation
- Ensuring that the school complies with safeguarding legislation, particularly in response to online safety and social media
- Receiving a yearly report on bullying incidents to include details of online safety issues

Head teacher and Senior Leaders

- Ensuring the safety of staff and students
- Ensuring that the online safety Policy, and its related procedures and strategies, are implemented, monitored and reviewed

- Ensuring that the DSL takes lead responsibility for online safety for the school but may delegate reporting, intervention or monitoring day-to-day to other members of the safeguarding team
- Ensuring that **all** staff are aware of their responsibilities
- Taking appropriate action against staff or students who breach the guidelines
- Ensuring that students, parents, staff and governors are regularly updated on e-safety guidance and messages, including in training of new staff, delivering assemblies or providing guidance during parents' evenings or through parent portal
- Collecting information on the numbers of incidents and reporting to Governors annually

Designated Safeguarding Lead

- Ensuring that safeguarding procedures are followed up appropriately in regard to online safety breaches or reports

Technical staff

- To ensure that the school's ICT infrastructure is secure and not open to misuse or malicious attack
- To ensure the school meets external technical requirements outlined in Trust Guidance, **South West Grid for Learning Security Policy** guidance and Acceptable Use policies
- Provide users access to the school's network through a properly enforced password protection policy in which passwords are regularly changed
- Ensuring that the school's filtering policy is applied and updated on a regular basis, and that its implementation is not the sole responsibility of any one single person
- To regularly monitor network/remote access in order to identify misuse or attempted misuse. This should then be reported to the DSL.
- To provide technical support to those investigating any breaches of acceptable use
- Monitoring software systems, such as Impero, are implemented and updated as appropriate
- To review classroom IT activity and report breaches

All staff, to include cover staff and ITT students

- Responsible for using the school's ICT system in accordance with the Staff Acceptable Use agreement (Appendix 2)
- To engage in appropriate training activities to update knowledge
- To read, sign and abide by acceptable use agreements
- To challenge and log any online safety related incident or acceptable use breach on Class Charts and send an email to alert the safeguarding team of any safeguarding matter
- To promote safe use of mobile devices and the internet
- To support the school's no mobile phone policy within the school and confiscate a phone if seen
- To keep their password secure and close down/lock devices when not in use
- To ensure that they will not invite, accept or engage in communications with parents or students within the school community in any personal social media
- To report any communication received from students on any personal social media sites to the DSL
- To report any inappropriate communications involving students or staff in any social media to the DSL/Headteacher
- To ensure their own privacy by using the highest privacy setting levels on all personal social media accounts
- To use email communications to parents, staff or students from official school accounts in an appropriate or acceptable manner

- To consider the reputation of the school in any posts or comments related to the school on any social media or on the internet
- To refuse requests from any current students or past students who are under eighteen as a friend, follower or subscriber (or similar) on any personal social media accounts
- To inform students about the risks associated with taking, sharing, publicising and distributing images, with or without consent
- To recognise the risks associated with sharing their own images via the internet or on social media
- To use digital imagery/video to support educational aims whilst following school guidelines in terms of consent of parents/carers
- To teach explicitly critical awareness of the materials/content that students access on-line and guide them to validate the accuracy of information from three independent sources, in particular misinformation and disinformation
- To teach students to acknowledge the source of information and to respect copyright
- To guide students (in lessons where internet use is pre-planned) to sites checked for suitability and to inform the IT Support if any unsuitable materials are found
- To use Impero or closely monitor students when “free” searches of the internet are suggested. Impero can be used to allow only specific sites and can block internet use completely
- Students’ work can only be published online with their permission and that of their parents/carers

Students

- Responsible for using the school IT systems in accordance with the Student Acceptable Use Agreement (Appendix 3). This will be signed and no access to the school system will be given without this consent
- To take care when sharing images online. Students must never use, share, publish or distribute images of others without their express permission
- To provide feedback to the school in support of developing Online safety strategies

Parents/Carers

- To support their children to adhere to the Student Acceptable Use agreement both within and outside of school
- Support school-based sanctions when agreements are broken
- To provide feedback to the school in support of developing Online safety strategies
- To sign parental agreement for child’s acceptable use on entry to the school

Community Users/ Visitors

- To agree to the Acceptable Use policy before being given access to the school systems

Additional issues

Training of staff and governors

- Routine training will be given to staff and governors to ensure they understand their responsibilities as outlined within the policy in line with Child Protection and Safeguarding procedures. All new staff will be trained during their induction period

Technical: infrastructure/ equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure is secured against physical attacks, accidental damage, and malicious software as is reasonably possible. Use of a firewall, antivirus software, physical restriction/filtering system is mandatory. There will be regular reviews and audits of safety and security of school systems
- All users will be provided with a user name and password by the IT Support who will keep up-to-date records of usernames, access rights and group memberships which will be reviewed at least annually
- The master administrator passwords will be used by **IT Support** but also must be available to the **Trust IT Manager**, Headteacher or nominated Senior Team member
- Filtering will be maintained by SWGfL and any staff requests to switch off the filtering/unblock sites will go through the following process. Short term (for example, 1 lesson/day) requests to HOF who will make the IT support request. Longer term requests (for example, unblocking of sites permanently) to be reviewed by the **IT Strategy group**.
- ICT staff will regularly monitor and record activity of users on the school network
- Temporary access for “guests” will be agreed via the IT Support request and the **IT Strategy group**

Recording Incidents

All Impero alerts and incidents should be recorded on CPOMS.

For incidents that involve bullying behaviours, specific categorisation is required on this system to recognise the roles of participants.

Breaches of the Policy

Breaches will be thoroughly investigated and school-based sanctions will apply, see Appendix 1.

Conclusion

The successful implementation of this policy will ensure that all members of the school community feel safe and secure (both physically and digitally) whilst at school.

Appendix 1: Grid for responses to misuse

A record of incidents will be held on Class Charts and/or CPOMS

	1 st incident	2 nd incident
C1 <ul style="list-style-type: none"> • Allowing other people to know your password • Allowing other people to use your account • Browsing the internet without permission • Playing games during lessons • Messaging students via email when not permitted to 	<ul style="list-style-type: none"> • Conversation with tutor/teacher as appropriate 	<ul style="list-style-type: none"> • Blocked from using system for one lesson/day/week as appropriate
C2 <ul style="list-style-type: none"> • Deliberately accessing/searching for inappropriate material on the internet, including using proxy servers to avoid school filtering Systems • Sending inappropriate emails • Using someone else's account/password 	<ul style="list-style-type: none"> • Teacher/pastoral detention 	<ul style="list-style-type: none"> • Blocked from using system for 1 week + after school detention
C3 <ul style="list-style-type: none"> • Taking ICT equipment apart • Viewing pornographic or offensive material • Minor damage to systems • Doing unauthorised administrative tasks 	<ul style="list-style-type: none"> • Blocked from using system for 1 week • After school detention • Recorded as a Child Protection incident, if appropriate 	<ul style="list-style-type: none"> • Blocked for longer period at discretion of DHT • Time in Reset Room • PCSO involved (where pornography/offensive materials) and recorded as a Child Protection incident • Liable for cost of damage
C4 <ul style="list-style-type: none"> • Unauthorised installation of software • Making system software unusable • Deliberate hacking/willful damage • Distribution of pornographic or harmful material 	<ul style="list-style-type: none"> • Blocked for longer period at discretion of DHT • Time in Reset Room • PCSO involved (where pornography/hacking) • Recorded as a Child Protection incident 	<ul style="list-style-type: none"> • Blocked from system at discretion of DHT • Suspension considered • Police involved and recorded as a Child Protection issue • Liable for cost of damage

Appendix 2: Acceptable Use policy for students

Students are responsible for good behaviour on the school network, email and the internet, just as they are in a classroom or a school corridor. General school rules therefore apply.

The following are not permitted:

- Using proxy servers to avoid school filtering systems
- The deliberate sending or displaying of offensive messages or pictures
- Using obscene language, harassing, insulting or attacking others. This kind of behaviour may result in being reported to the police
- Sending of files/attachments to emails which are not decent
- Transmitting of materials which are offensive or not connected with school
- Violating copyright laws
- Using Artificial Intelligence to produce work and not stating the source used
- Using others' passwords or accounts
- Using chat lines, chat applications and message sending platforms
- Trespassing in others' folders, work or files including system "out of bounds areas"
- Intentionally wasting resources (only download, save or print items which are for classwork, project or coursework/controlled assessment purposes)
- USB sticks/downloads containing programs must not be used on or loaded onto the school computers (data files, word processed text may be uploaded with permission)

As a user of the school network, the internet and email, I agree to comply with the school rules on their use. I will use the network, internet and email in a responsible way and observe all the restrictions detailed in the acceptable use policies.

Signed

Date_

As a parent/ carer, I agree to my child following the Acceptable Use Policy.

Signed

Date_

Social media guidelines

When using social media for educational purposes, the following practices will be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff and should ideally be linked to an official school email account. The form **CSSSubject** is preferred
- The URL and identity of the site should be agreed with the Head of Faculty before access is permitted to students
- The content of school social media sites should be solely professional and should reflect well on the school
- Staff must not publish photographs of students without reference to the consent of parents/carers, or identify any students directly with full names or allow personal information to be published on these sites
- Care must be taken that any links to external sites from accounts are appropriate and safe
- Any inappropriate comments on or abuse of school-sanctioned social media should be reported immediately to the SLT link or DSL
- Staff should not engage in any direct messages with students through social media where the message is not public
- Students can be friends, followers, subscribers on school sanctioned social media sites but staff will not follow students/profiles

Mobile Technologies Use guidelines

If staff wish to use their own mobile or portable devices such as ipads, mobile phones within the school wireless system, they should contact IT support who will configure access settings for the school network. If staff have visitors who require guest wireless access, staff should complete an IT Support request.

Data Protection guidance

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

- **Lawfulness, fairness, and transparency:** Data must be processed legally, fairly, and in a transparent manner in relation to the data subject.
- **Purpose limitation:** Data must be collected for specified, explicit, and legitimate purposes and not processed further in a manner incompatible with those purposes.
- **Data minimisation:** Data collection must be adequate, relevant, and limited to what is necessary for the intended purposes.
- **Accuracy:** Personal data must be accurate and kept up to date; inaccurate data should be erased or rectified.
- **Storage limitation:** Data should only be kept for as long as necessary, in a form that allows identification of data subjects for no longer than is required.
- **Integrity and confidentiality (security):** Data must be processed securely, with appropriate technical or organisational measures to protect against unauthorized access, loss, or damage.
- **Accountability:** The data controller is responsible for complying with these principles and must be able to demonstrate compliance