Online Safety Policy
Sept 2024

To be reviewed
Sept 2025

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of digital technologies.
- Safeguard and protect students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of the school community - staff, students, governors, volunteers, parents and carers, visitors, community users - who have access to and are users of the school's ICT systems.

Communication of the policy

The policy will be communicated to the school community in the following ways:

- Displayed on the school website, and available in the staffroom.
- Included as part of the induction pack for new staff alongside staff agreement.

Responding to complaints

- The school will take all reasonable precautions to ensure online safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school, or Local Authority, can accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed as part of their Internet Safety module of the risks and safety measures they need to take whilst accessing the internet in school.
- Any complaint or concern will be dealt with by SLT and reported to the necessary members of staff. Any complaint about staff misuse will be referred to the Headteacher.
- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the school child protection procedure. (See Child Protection and Safeguarding Policy)

Review and Monitoring

Online safety is integral to other school policies including the Child Protection and Safeguarding Policy, GDPR Policy, Induction of New Staff and Anti-Bullying Policy.

The school's online safety coordinator is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and/or circumstances and online safety issues in the school. Staff and Governors will be informed of any updates or amendments to it.

2. Education and Curriculum

Student online safety curriculum

The school has a clear, progressive online safety education programme primarily as part of the Computing curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy including critical thinking and identifying misinformation online.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Recognising and reporting concerns or abuse.
- Positive relationships.
- Laws around online behaviour (Prevent Duty and Sexting Guidance for schools)

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the lock screen message they see when accessing any mobile school device.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.
- Staff training.
- Safe delivery of remote learning when the school is closed or students are accessing lessons remotely and ensure that acceptable behaviours as outlined in the Remote Learning policy are adhered to.

The school will ensure that:

- Staff are provided with updated information on how the GDPR and Data Protection Act affect the way data is collected and stored at school.
- Staff understand the requirements of the GDPR and Data Protection Act in terms of sending and receiving sensitive personal information.
- All sensitive and confidential information should be securely stored and password protected.

- Regular training is available to staff on online safety issues and the school's online safety education programme.
- Information and guidance on the Safeguarding policy (including updates to Prevent Duty guidance and Keeping Children Safe in Education is provided to all staff and governors at least annually.

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face or online sessions to support parents in developing their child's/children's digital resilience
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

3. Conduct and Incident management

Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Agreements they have signed. They should understand the consequences of misuse, or accessing inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the school's Misuse Incident Policy. The school actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about students.

4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- All staff users will be provided with a username and secure password. Users will be responsible for the security of their username and password.
- All pupils have multiple username and passwords for school approved learning tools. Staff manage and are responsible for updating and resetting passwords.
- Internet access is filtered by Smoothwall but managed by our Network Manager for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school allows different filtering levels for staff and students.
- The school regularly monitors and records the activity of users on the school technical systems and this extends to the use of school-owned devices when being used remotely and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for users to report any technical incident or security breach.
- The school infrastructure is protected by up to date anti-virus software where necessary and backed up regularly.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Social Media

The school has a Social Media Policy that covers the management of school accounts and the guidelines for staff, students and parents' personal use of social media.

5. Data

The school has a GPDR data Protection Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the

responsibilities of the Senior Information Risk Officer (SIRO); and the storage and access of data.

Where schools allow the use of staff personal devices to be used for school work, the following can be included:

There is a policy outlining when and how staff may use their own devices for work purposes and this includes the handling of personal data and sensitive information.

6. Equipment and Digital Content

Use of Mobile Technologies

Personal mobile phones and mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal mobile phones or other internet enabled devices which are brought into school.

Staff Use

Staff are permitted to use their own mobile phones and they can be connected to the school network. No images are permitted to be taken on personal devices. Parents may be contacted through the school emails and Teachers to Parents. Video calling may be used for remote face to face contact using a school device.

Mobile phones and other devices will be switched off or switched to 'silent' mode. Mobile phones or other personal devices will not be used during teaching periods.

Staff should not use their own devices such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Where staff are required to use a mobile phone for school duties – e.g. in case of emergency during off-site activities, or for contacting students or parents - they should use their own device and hide their own number (by dialling 141 first).

Digital images and video

We will seek permission from parents and carers for the use of digital photographs or video involving their child as part of the permissions form completed when their child joins the school.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.

7. Links to other policies

This online safety policy is linked to our:

Acceptable Use Agreements

Anti-bullying policy

Child protection and safeguarding policy

GDPR Data protection and handling policy

Remote Learning Policy

Social Media Policy

Induction of New Staff

8. Useful Contacts

Headteacher

Designated Safeguarding Lead

Network Manager