Online Safety Policy

Written April 2016
Reviewed February 2021

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 ICT
- Safeguard and protect the 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 school community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of 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
- Included as part of the induction pack for new staff
- Acceptable use agreements discussed with and signed by students at the start of each year
- Acceptable use agreements to be held in student and/or personnel files

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 nor the Local Authority can accept liability for material accessed, or any consequences of internet access
- Staff and students are informed of the possible sanctions related to misuse of technology
- Our online safety coordinator is the first point of contact for any complaint. 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.

Review and Monitoring
Online safety is integral to other school policies including Computing Policy, Safeguarding Policy, Anti-Bullying Policy, Behaviour Policy and Remote Learning Policy.

The policy will be reviewed annually or more frequently in response to changing technology and online safety issues in the school.

This policy has been approved by the Senior Leadership Team and Board of Governors. Staff 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
- Acceptable online behaviour
- Understanding online risks
- Privacy and security
- Reporting concerns

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 Acceptable Use Policy signed by every student
- 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 and governor training
The school will ensure that:

- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information
- Regular training is available to staff on online safety issues and the school's online safety education programme

- Information and guidance on safeguarding and the school's Acceptable Use Policy is provided to all new staff and governors.

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
- Support and advice on online safety for their children outside of school through in person workshops
- 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 Policy they have signed. They should understand the consequences of misuse or access to 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 Plan. 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.

All incidents should be reported immediately to the Designated Safeguarding Lead (DSL). Incidents will be reported to the police by the DSL as appropriate.

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
- Each student will have their own log on credentials
- Internet access is filtered for all users. Illegal or inappropriate content is filtered by the broadband and/or filtering provider (LGfL)
- The school allows different filtering levels for different groups of users –staff / students
- There is a reporting system in place for users to report any technical incident or security breach through NPW and DSL via safeguard or e mail.
- Security measures are in place protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- All staff should make use of an encrypted USB which is provided by the school or save work on password protected google drive.

Social Media
The school has a Social Media Policy that covers the management of school accounts and set out guidelines for staff personal use of social media.

5. GDPR

The school has a GDPR Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Senior Information Risk Officer; and the storage and access of data.

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

Personal mobile phones and mobile devices
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 mobile devices.

Student Us
Any students bringing in phones for safety purposes will be stored with the staff in the school reception for the duration of the day.

Staff Use
Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and 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 - then a school mobile phone will be provided. In an emergency where staff do not have access to a school device, 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 Use of Digital and Video Images Agreement 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 online 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. Prevent duty

The latest research shows that up to 90% of radicalisation occurs through social media and other online platforms. All children at a primary stage do not meet the age requirement for using social media platforms, for this reason, our filtering policy blocks all requests to social media platforms made by students. Staff are able to unblock certain websites for educational purposes, such as YouTube but other sites such as Facebook are blocked for staff also.

We understand that it is more beneficial to educate children about online safety as opposed to blocking them from everything, especially as we have little control over what they are exposed to via their home internet. Therefore, as part of the computing curriculum, class teachers run regular online safety lessons which progress through the key stages. All KS2 children also have access to CyberPass (by LGfL) which allows children to deepen their understanding in online safety.

We also have Use Acceptable Policies (UAP) for both students and staff to ensure that everyone using the internet by connecting to our WiFi/wired connection understand their responsibilities.

Links to other Policies:

- Computing
- Remote Learning
- Safeguarding