FACT

01689842268

www.factrust.org

Online Safety Policy

Reviewed: June 2024

Next review: June 2025

Rationale

"It is essential that children are safeguarded from potentially harmful and inappropriate online material".

'Keeping Children Safe In Education,' 2022

The school's online safety policy will be mindful of and raise awareness of the four key areas of risk:
Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying
Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Aims and Objectives

The purpose of this policy is to set out the procedures by which the school will minimise the misuse of computers and associative technology.

- To ensure that the school acts within the requirements of the General Data Protection Regulation (GDPR) when retaining, storing and sharing personal data.
- To ensure that the process of responding to enquiries for other information is also legal under the Freedom of Information Act 2000.
- To empower the whole school community with the knowledge to stay safe and risk free.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to the student or liability to the school.
- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body and parents.

Teaching and Learning

Online safety is taught in all year groups as an embedded and regular part of the school's computing curriculum, and as part of PSHE. The topics in online safety lessons cover a wide variety of contexts people face online, including website content, filters for content, conversations with others online, online scams and reliability of sources. The school also participates in Safer Internet Day every year, revising skills to stay safe online and to continue to raise awareness across all Key Stages.

General Use of Computers

- The use of school computers will be permitted only for purposes directed by the school.
- Pupils will be taught to be critically aware of the materials they read online and where to look for information appropriate for their age group.
- Users are not permitted to access and amend another user's work without permission.
- All computers connected to the internet will be protected by anti-virus software which will be kept up to date to check for the latest viruses.
- No files should be brought in from home and loaded on the school system without permission from the teacher.
- The school reserves the right to look at any files on their system including text, graphics and e-mails.
- The school reserves the right to deny access to school computer systems.

Infringements

- Any infringements of Online safety should be logged onto the CPOMs system, which will alert the schools designated safeguarding officers and report to the senior management where further action can be taken if required.
- Staff are responsible for their digital footprint online and should act accordingly. Any misuse of social media involving the school could lead to disciplinary action. (See the Social Media Policy)

Internet Access

- The school provides Internet access for educational purposes and should only be used by staff, pupils and members of the community for these purposes.
- The school connects to the Internet via a filtered service. Pupils cannot use computers without filtered access. The school monitors and adjusts the filter as appropriate.
- All Internet access by pupils is supervised by a member of staff or other responsible adult.
- No pupil, member of staff or community user is permitted to access material that is illegal or potentially offensive using school systems.
- The copyright and intellectual property rights of material using the school system will be respected.
- Professional e-mail correspondence will only be conducted via school e-mail addresses.
- The school does not use any pictures, videos or audio files on its online presence without prior permission from parents/carers.
- Like health and safety, Online safety is the responsibility of everyone to everyone. As such everyone will promote positive Online safety messages in all use of IT whether with other members of staff or with students.
- Access to social media sites are blocked by the network filter within school.
- Staff and those working within the school, using social networking for personal use, should never undermine the school, its staff, parents or children.
- Staff should think carefully before allowing parents of pupils to become their "friends" on social media.

Devices

The school does not condone the underage use of social media applications, but recognises that some parents/carers choose to allow their children access to these. The safe use of age-appropriate applications will be taught in online safety lessons.
Parents will be offered guidance on how to set parental controls on devices and keep their children safe online. We will regularly send parents "What you need to know," guidance on specific apps, from National College Online Safety.

Children are not allowed to use devices on the school site. Children below Year 5 are not allowed to bring devices to school and we strongly discourage parents and carers from allowing older children to bring devices. This includes SMART Phones, SMART watches and tablets. For further information, see the school's Mobile/Smart Phone Policy.

Staff will only use personal devices when they are not in contact with children. These devices will be kept safely away from children.

- All use of personal devices to take pictures, videos or audio files in school should be avoided. However, if personal devices have been used in school, any images taken should be uploaded to the Google Drive and deleted from the original device (ideally in the presence of another member of staff).
- Any new devices within the school will be subject to a risk assessment to identify the appropriate use in school.

Filtering and Monitoring/Evaluation

Monitoring of internet use in school is managed through LGfL's filtering service, called 'School protect' This service has a default list of websites and categories (regularly updated by LGfL) which are blocked for all schools. The school administrator also has the option to block/unblock other websites as needed.
Another system, Securly, is used to apply filtering to the school's Chromebooks. This works in a similar way to School Protect but the filtering is also applied to the device if it is being used outside of school (which supports safe internet use during remote learning). Securely sends a message directly to the DSL's should a child try to access a blocked site.
The effectiveness of the school's online safety is monitored by the SLT using the '360 Safe,' self-monitoring tool.

Remote Learning

When learning is being accessed remotely, all work is provided through Google Classroom, with contact between teachers, parents and pupils being only through the year group email address. When live lessons are being conducted, a member of the SLT will sit in on the session. For further information, see the school's remote learning policy.

Mental Health and Wellbeing

Children's online safety lessons will focus on staying safe online, but also look at how our behaviour online and use of devices can affect our mental health and wellbeing. This is linked closely to the school's mental health and wellbeing review conducted by the senior leadership team.