ST GABRIEL'S
NEWBURY

E-Safety Policy

Including our Early Years Foundation Stage

Authorised by	resolution of the Board of Governors
Date	Autumn 2023 (1-0-0) Autumn 2024 (1-0-1)

St Gabriel's is committed to safeguarding the children and young people with its care, especially when they are using the internet, social media, or mobile devices.

The purpose of this policy statement is to:

- provide staff and volunteers with the overarching principles that guide our approach to online safety
- To ensure that pupils are appropriately supervised during school activities.
- To promote responsible behaviour with regard to e-based activities.
- ensure that, as a school, we operate in line with our values and within the law in terms of how we use online devices. This includes the General Data Protection Regulations and the Data Protection Act 2018.

This policy applies to pupils, staff and volunteers, and others using the school's ICT services.

This policy has been written in accordance with

- Keeping Children Safe in Education 2024
- Preventing and tackling bullying 2017
- Searching, Screening and Confiscation 2022
- Cyberbullying: Advice for headteachers and school staff
- Meeting digital and technology standards in school and colleges (updated March 2023)

Responsibilities

The Principal will be responsible for the implementation of this policy and will report on filtering and monitoring to the Safeguarding Governor, who will act as the responsible governor.

The Bursar will act as E-Safety Coordinator and will (in conjunction with the Designated Safeguarding Lead and Head of Compliance)

- compile logs of e-safety incidents;
- report to the Principal on recorded incidents;
- ensure that staff are aware of this guidance;
- provide / arrange for staff training;
- liaise with school technical staff;
- liaise with the Principal on any investigation and action in relation to e-incidents; and
- Instigate a regular (I.e. at least annually) review of filtering and monitoring, and online safety. Ensure that the school's ICT support services
    - are responsible for the IT infrastructure and that it is not open to misuse or malicious attack;
    - ensure that users may only access the networks and devices through an enforced password protection policy;
    - keep up to date with e-safety technical information in order to carry out their role;
    - ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse; and
    - implement any agreed monitoring software / systems ensuring that it has the technical requirements to meet government standards as detailed in Meeting digital and technology standards in schools (updated March 2023).

The Designated Safeguarding Lead as a member of the School's Senior Leadership Team will

- take lead responsibility for understanding the filtering and monitoring systems and processes in place.
- Also review filtering and monitoring reports
- Respond to safeguarding and online safety concerns
- Support staff to give parents information about how to keep their children safe online

Teaching and Support Staff will

- maintain awareness of school e-safety policies and practices through training on the expectations and roles and responsibilities in relation to filtering and monitoring; This should give them an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- report any suspected misuse or problem to the Principal or the Bursar
- ensure that all digital communications with pupils, parents and other staff are on a professional level and conducted on school systems;
- where relevant, e-safety is recognised in teaching activities and curriculum delivery;
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism, including through the use of AI and uphold copyright regulations;

- monitor the use of digital technologies (including mobile devices, cameras etc during school activities); and
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Review Process

The review should be conducted by the Bursar, the DSL and the school's ICT support service. The responsible governor should also be involved. The results of this review will be recorded. A review will also take place when

- A safeguarding risk is identified
- There is a change in working practice, such enabling remote access or BYOD or the use of AI
- New technology is introduced.

The review will identify current provision, any new requirements, and will reflect the needs of pupils and staff. The review will consider

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of our pupils
- teaching requirements including the RSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

The results of the review will inform

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

Other E-Safety Measures

Pupils and staff / volunteers sign Use of Technology agreement before accessing school systems. Pupils understand that e-safety and Use of Technology conditions apply to actions outside of school where related to school activities.

At the beginning of the school year (and periodically during the year) the school will provide information to parents about keeping their children safe online. In addition, parents are given guidelines on the use of digital and video images taken at school events.

Pupils, as part of the wider curriculum, including PSHE programme and computing lessons are taught about

- personal information and its security,
- The effective use of passwords and log ons
- Using the internet and mobile phones in a way that keeps them safe and shows respect for others including information about grooming and cyberbullying
- How to report abuse, misuse or access to inappropriate materials

This policy should be read in conjunction with

- Child Protection (Safeguarding) Policy
- Anti-Bullying Policy
- Technology Use for Pupils
- Technology Use for Staff

Date	Version	Changes
Autumn 2023	1-0-0	Policy written as a standalone policy, rather than a sub policy of Child Protection
Autumn 2024	1-0-1	Refer to Technology Use agreement KCSIE 2024