ALL SAINTS' CE PRIMARY SCHOOL

ONLINE LEARNING AND SAFETY POLICY

2023/2024

Approved by	
Name:	Grace Bennion
Position:	Chair of Governors
Signed:	
Date:	16th October 2023
Review date:	September 2024 or sooner if required

Introduction

Online safety, also known as e-safety, relates to the protection of school children when they are using the internet and electronic devices. Given the increasing role of online learning, it is essential to have an integrated approach towards online safety and online learning.

Aims

- To provide a safe online environment for all students.
- To equip students with the skills and knowledge to use the internet safely and responsibly.
- To ensure that online learning is effective and does not compromise the safety or wellbeing of students.

Safe and Acceptable Use of Technology

All school computers and online systems will have updated anti-virus and security software. The school will use a filtered internet service to block inappropriate content. Personal devices may only be used if they meet the school's security requirements (see BYOD policy). All members of the community should use any school devices or accounts appropriately. For staff, acceptable use forms part of professional standards and is part of their contract. All new members of staff will be given resources to access accounts and informed of expectations for acceptable use. Personal data will be handled in accordance with the Data Protection Act and GDPR. Teachers will ensure virtual classrooms or forums are moderated and monitored.

Bring Your Own Device (BYOD) Policy

All staff, whilst in school, should use devices provided for them for day-to-day use. On occasions, there may be a need for a member of staff to use a personal device within the school. If this is the case, it should be done so through the authorisation of the Headteacher, on a request basis. The filtering and monitoring system employed by the school is suitably robust enough to prevent mobile phones from causing disturbance or threat to the school's online platforms and they are, in many respects, important devices we rely on for safeguarding and communication. However, they should not be used during lesson time. Visitors to the school requesting access to the school's internet may do so with approval from a member of the core staff team (comprising the Headteacher, office staff and the teaching and learning team). This will purely allow access to the school's Wi-Fi and will in now way give access to the school's online platform. Requests to use external memory storage devices on a school device will normally not be accepted but may be sanctioned by the Headteacher in exceptional circumstances.

Digital Literacy and Curriculum

E-safety will be integrated into the curriculum where children are taught about the benefits, risks and responsibilities of using technology. It is important for us to teach the children about responsible searching using search engines (such as Swiggle). This will be done as part of our e-safety module, where we look at topics such as safe searching, trusted sources of information, etc.

Regular workshops and awareness campaigns for students on topics like cyberbullying, sharing personal information and understanding digital footprints.

Website and YouTube videos being used in lessons should be researched and vetted by staff before use. YouTube should only be unfiltered on staff devices and devices that children use should be limited to YouTube Kids results by IP address.

File Management

All staff are provided with unlimited file storage, accessible with an internet connection, both in school and remotely. Staff are encouraged to manage their personal filing system to ensure ease of access of their files. Staff have access to, and are encouraged to use, shared drives within the school's domain.

They should work with other staff to ensure they are well managed and organised, informing colleagues of any major changes to the file organization system. The file storage system should be used exclusively for work purposes.

Students all have their own unlimited file storage space. Shared files are also accessible to students. These can be shared by staff or between students. Staff should encourage students to manage and organise their files and folders appropriately and respect the privacy of other user's data.

Reporting and Handling Issues

An e-safety coordinator will be designated in the school (Ashley Ryan).

Students are encouraged to report any online concerns or issues to their teachers.

A clear protocol will be in place to handle and escalate any e-safety incidents.

Learning Platforms

Only approved online learning platforms will be used both in a school setting, for setting homework and in the event of online learning and homeschooling. Approved platforms for setting work are Microsoft 365 and Class Dojo. Apps such as Spelling Shed and TT Rockstars can also be used as part of the children's homework.

Behaviour and Etiquette

Students are expected to maintain the same behaviour online as they would in a physical classroom. Any incidents of cyberbullying or inappropriate behavior will be dealt with in line with the school's behavior policy.

Access and Equity

The school will take steps to ensure that all students have equal access to online learning resources, considering factors like technological barriers or special educational needs.

Materials should be printed in formats that are accessible to all students, including those with disabilities.

Communication with Parents

Parents will be informed about the online tools and platforms used by the school. E-safety guidance and resources will be regularly shared with parents. Parents will be encouraged to monitor their child's online activities and to discuss online safety at home. Only approved platforms should be used to communicate with parents (Microsoft 365 and Class Dojo) and social media should not be used to communicate matters involving the school or children.

Staff Training

Regular training sessions will be conducted for staff on online safety and online learning best practices.

Staff will be made aware of the procedures to follow in the event of an e-safety incident.

Policy Review

This policy will be reviewed annually or in response to significant online safety updates or incidents. Feedback from students, staff and parents will be considered in the review process.

Online Safety Policy for All Saints' CE Primary School

1. Introduction

All Saints' CE Primary School is committed to creating a safe and secure digital environment for all students, staff and visitors. This policy outlines the school's approach to online safety and is written in line with the requirements of the Department for Education's Keeping Children Safe in Education guidelines (KCSiE), especially its references to monitoring and filtering digital technologies to ensure responsible and appropriate use.

2. Aims and Objectives of this policy

- To protect students from exposure to harmful or inappropriate online content.
- To ensure compliance with legal requirements and relevant standards regarding digital and technology use in schools, specifically within the Keeping Children Safe in Education (KCSiE) guidelines (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) and the Department for Education's Meeting Digital and Technology Standards in School and Colleges (https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges)
- To promote responsible internet use and digital citizenship among students and staff.
- To maintain a secure network infrastructure and protect against potential threats or unauthorised access.
- To provide support and guidance for users in navigating digital technologies safely and effectively.
- Monitoring and filtering systems, roles and responsibilities are detailed in Appendix 1.

3. Identifying and assigning roles and responsibilities to manage filtering and monitoring systems

The Governing Board has overall strategic responsibility for filtering and monitoring and needs assurance that the standards are being met. To fulfil this, the following is in place:

- member of the Senior Leadership Team and Governor, to be responsible for ensuring these standards are met
- Nicola Smallwood, Headteacher
- Liz Pritchard, Safeguarding Governor
- roles and responsibilities of staff and third parties, for example, external service providers

The Senior Leadership Team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of our provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

As Designated Safeguarding Lead (DSL), the Headteacher works closely with governors and our external IT service providers in all aspects of filtering and monitoring.

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The Headteacher works closely together with IT service providers to meet the needs of our setting.

The Headteacher takes lead responsibility for safeguarding and online safety, in the following areas:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The Headteacher/IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks for systems

The Headteacher and IT service provider work to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

4. Review of filtering and monitoring provision

For filtering and monitoring to be effective it should meet the needs of students and staff and reflect specific use of technology while minimising potential harms. To understand and evaluate the changing needs and potential risks of our school, the filtering the monitoring provision is reviewed at least annually.

Additional checks to filtering and monitoring are informed by the review process so that the governing body has assurance that systems are working effectively and meeting safeguarding obligations. Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually. The review is conducted by the Headteacher and the IT service provider where necessary and the responsible governor is informed/involved as necessary. The results of the online safety review are recorded for reference and made available to those entitled to inspect that information.

Technical requirements:

A review of filtering and monitoring is carried out to identify current provision, any gaps, and the specific need of our students and staff. This includes:

- the risk profile of our students, including their age range, students with special educational needs and disability (SEND), students with English as an additional language (EAL)
- what our 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 students
- teaching requirements, for example, our RHSE and PSHE curriculum
- the specific use of our chosen technologies, including Bring Your Own Device (BYOD)
- the related safeguarding or technology policies we have in place
- the checks that are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review informs:
- 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

The review is done annually, or when:
- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

When checking filtering and monitoring systems, we will make sure that the system setup has not changed or been deactivated. The checks will include a range of:
- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers; students and guests

A log of checks will be kept so they can be reviewed.

We will record:
- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

The Headteacher will make sure that:
- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and students
- block lists are reviewed and they can be modified in line with changes to safeguarding risks

The South West Grid for Learning's (SWGfL) testing tool is used to check that our filtering system is blocking access to:
- illegal child sexual abuse material
- unlawful terrorist content
- adult content

5. Blocking harmful and inappropriate content, without unreasonably impacting teaching and learning

The importance of meeting the standard: An active and well-managed filtering system is an important part of providing a safe environment for students to learn. No filtering system can be 100% effective. We understand the coverage of our filtering systems, any limitations it has, and mitigate accordingly to minimise harm and meet our statutory requirements in Keeping Children Safe in Education (KCSiE) and the Prevent duty.

Our filtering system blocks internet access to harmful sites and inappropriate content. It does not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

Our filtering system is operational, up-to-date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

Our filtering system:

- filters all internet feeds, including any backup connections
- is age and ability appropriate for the users and is suitable for our setting
- handles multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around filtering such as VPNs and proxy services and block them
- provides alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. If our users access content in this way, we should get confirmation from our provider as to whether they can provide filtering on mobile or app technologies. An appropriate monitoring system is applied to devices using mobile or app content to reduce risk of harm.

It is important to able to identify individuals who might be trying to access unsuitable or illegal materials so they can be supported by appropriate staff, such as the Senior Leadership Team or the Designated Safeguarding Lead.

Our filtering systems should allow us to identify:

- device name or ID, IP address and, where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

The school conducts its own data protection impact assessment (DPIA) and reviews the privacy notices of third-party providers. The Headteacher enforces Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for our users on top of the filtering service.

All staff are aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

6. The school has effective monitoring strategies that meet the safeguarding needs of the school

The importance of meeting the standard: Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows the school to review user activity on our devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome. Our monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies are required to minimise safeguarding risks on internet connected devices and include:

- physical monitoring by staff watching screens of users
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services. See Appendix 1 for further detail on this

Meeting the standard: The Governing Board supports the Senior Leadership Team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school. The Headteacher takes lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. The management of technical monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. Training is accessed to make sure knowledge is current.

Technical requirements and how the school meets the standard:

The Governing Board supports the Senior Leadership Team to review the effectiveness of our monitoring strategies and reporting process. We will always make sure that incidents are urgently picked up, acted upon and outcomes are recorded. Incidents could be of a malicious, technical or safeguarding nature. It is clear to all staff how to deal with these incidents and who should lead on any actions.

Device monitoring is managed by the Headteacher and external third-party providers, they:

- make sure monitoring systems are working as expected
- provide reporting on student device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

They also make sure that:

- monitoring data is received in a format that staff can understand
- users are identifiable to the school so concerns can be traced back to an individual, including guest accounts

Our active monitoring provision, Senso, identifies and alerts the Headteacher to behaviours associated with them:

- 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: 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 or financial scams. If we feel our students or staff are at risk, it will be reported to the Anti-Phishing Working Group (https://apwg.org)

The school acknowledges that technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

Appendix 1

Core school responsibilities for Monitoring and Filtering

Headteacher: Nicola Smallwood

Designated Safeguarding Lead: Nicola Smallwood

Data Protection Officer: Matthew Charters

Named person responsible for Monitoring and Filtering: Nicola Smallwood

E-Safety Coordinator: Ashley Ryan

School IT Support: Managed internally in conjunction with System IT Services

Monitoring systems

- physical monitoring by staff watching screens of users:
- comprehensive training is given to all staff to ensure that they are able to do this and are aware of their responsibilities
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Filtering Systems

- principal system provided by Fortinet, through Cumbria ICT who are a member of Internet Watch Foundation (IWF).

Person/department responsible for this: Nicola Smallwood, Headteacher