Growing together, hand in hand

Online Safety Policy

September 2024

Audience:	Staff/Governors/Public
Frequency of Review:	Annually
Post-holder responsible for Review:	Designated Safeguarding Lead and Digital Learning Lead

Introduction

This Online Safety Policy outlines the commitment of Gorsemoor Primary School to safeguard members of our school community online in accordance with statutory guidance including Keeping Children Safe in Education (2024) and Teaching Online Safety in Schools (2023) and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Policy Development, Monitoring and Review

This Online Safety Policy has been reviewed by the following:

- Co-Headteachers
- Designated safeguarding lead (DSL)
- Digital Learning Lead
- Pupil Entitlement and PSHE Lead
- Governors

Schedule for development, monitoring and review:

This Online Safety Policy was approved by the *school governing body on:*	*September 2024*
The implementation of this Online Safety Policy will be monitored by:	Designated Safeguarding Lead Digital Learning Lead
Monitoring will take place at regular intervals:	Annually
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2025
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Hayley Porter DSL* *Emilie Lees Co-Headteacher* *Nicky Costello Co-Headteacher*

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
  - learners
  - parents and carers
  - staff

Responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Co-Headteachers

- The Co-Headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Co-Headteachers are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Co-Headteachers are responsible for ensuring that the Designated Safeguarding Lead / Digital Learning Lead, IT service providers, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Co-Headteachers ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Co-Headteachers will receive regular monitoring reports from the Designated Safeguarding Lead.
- The Co-Headteachers will work with the Safeguarding Governor, the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
This review will be carried out by the governing board whose members will receive regular information about online safety in school via the DSL. The Safeguarding Link Governor will undertake additional responsibilities including:

- regular meetings with the Designated Safeguarding Lead / Digital Learning Lead
- regular receipt of (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to the Full Governing Board via link-governor reports and during Full Governing Board meetings
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role, following the KSCIE framework.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the link safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to the Co-Headteachers
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Digital Learning Lead

The DLL will:

- work closely with the Designated Safeguarding Leads (DSL) - the DLL is also a DDSL.
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are addressed to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies, including annual policy/document updates alongside the DSL.
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with PSHE lead to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:

– **content**
– **contact**
– **conduct**
– **commerce**

PSHE Lead

Curriculum Lead for PSHE will work with the DSL/DLL to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme (Project Evolve)
- PHSE and RSE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

IT Service Provider

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and technical security to carry out their work effectively
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority.
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement.
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance, local safeguarding policies and the remote learning policy.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

The school will take every opportunity to help parents and carers understand issues relating to online safety through:

- publishing the school Online Safety Policy on the school website
- after-school workshops ran by lead by the Digital Learning Lead
- publishing copies of the learners' acceptable use agreements on the school website
- publishing information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user Acceptable Use Agreement before being provided with access to school systems.

Gorsemoor Primary School encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Acceptable Use, Reporting and Responding

Acceptable Use

The Online Safety Policy and acceptable use agreements define acceptable use at Gorsemoor. The acceptable use agreements will be communicated and re-enforced through:

- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- the curriculum
- school website
- peer support

Acceptable use agreements for Key Stage 1 and 2, staff and volunteers, and parents/carers can be found under 'policies' on our school website.

Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead and SLT have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Co-Headteachers, unless the concern involves the Co-Headteachers, in which case the complaint is referred to the Chair of Governors and the local authority.
- where there is no suspected illegal activity, devices may be checked by SLT.

Online Safety Education at Gorsemoor

Online safety is a focus in all areas and staff reinforce online safety messages across the curriculum. Our online safety curriculum is broad, relevant and provides progression and creativity, and is provided in the following ways:

- A planned online safety curriculum for all year groups matched against nationally agreed frameworks such as the Education for a Connected World Framework by UKCIS/DCMS and SWGfL Project Evolve and are regularly taught in a variety of contexts
- Objectives are linked to the RSE curriculum
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g., PHSE; SRE; Literacy etc.
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- The online safety education programme is relevant and up to date to ensure the quality of learning and outcomes.
- Topical issues are also addressed and taught via responsive lessons, discussions and workshops such as the increasing risks of Artificial Intelligence and steps to safeguard themselves around this.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school

community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- Mechanisms to canvass learner feedback and opinion through pupil voice
- Appointment of digital learning ambassadors
- Contributing to online safety events with the wider school community such as our open evenings.

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and our IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL has lead responsibility for safeguarding and online safety and our IT service provider has technical responsibility.

Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- Access to content through non-browser services (e.g., apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Technical Security

The school technical systems are managed in ways that ensure the school meets recommended technical requirements.

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by SLT.
- Password policy and procedures are implemented through the acceptable use agreements signed by staff/volunteers.

- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication (MFA).
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and system will be protected by secure passwords.
- The administrator passwords for school systems are kept in a secure place, e.g., school safe.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- Appropriate security measures are to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The IT provider is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to SLT
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- Staff members are not permitted to install software on a school-owned devices without the consent of SLT/IT service provider
- Removable media is not permitted unless approved by SLT
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place via mobile device management software.

Data Protection

The school:

- Has an SLA with Entrust that provides the school with information governance, including:
  - Information and cyber security
  - Data Protection
  - Freedom of Information
- implements the data protection principles and can demonstrate that it does so
- Has appointed the Office Manager as Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- Has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- Has procedures in place to deal with the individual rights of the data subject
- Carries out Data Protection Impact Assessments (DPIA) where necessary
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff
- When personal data is stored on any mobile device or removable media the:
  - device will be password protected.
  - device will be protected by up-to-date endpoint (anti-virus) software
  - data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
  - data will be encrypted, and password protected.
- Staff must ensure that they:
  - at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
  - can recognise a possible breach, understand the need for urgency and know who to report it to within the school
  - can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
  - only use encrypted data storage for personal data
  - will not transfer any school personal data to personal devices.
  - use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
  - Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- Staff are well informed of the digital world and the risks associated with technology