Goonhavern Primary School

Online Safety Policy 2023/24

This policy applies to all members of the school community (including staff, learners, 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).

Date created: November 2023

Next review date: September 2024

Next review date: March 2025

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Goonhavern Primary School to safeguard members of our school community online in accordance with statutory guidance 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).

Goonhavern Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review This

Online Safety Policy has been developed by the Online Safety Group made up of:

- *Gary Jones (headteacher/ Designated safeguarding lead*
- *Martin Borrott (Assistant Headteacher, Online Safety Lead)*
- *Lucy Gibson (Computing Lead)*
- *Edd Bissenden (Online Safety Governor)*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*20.02.24*
The implementation of this Online Safety Policy will be monitored by: Martin Borrott	Martin Borrott
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 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Martin Borrott, Gary Jones, Martin Davis, Edd Bissenden, Jacob Jones (DNS)

Process for monitoring the impact of the Online Safety Policy

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:*
  - o *learners*
  - o *parents and carers*
  - o *staff.*

Policy and leadership

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.

Headteacher and senior leaders

- The headteacher has 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 headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, 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 headteacher/senior leaders will 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 headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing

Body".

Link:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_d
ata/file/1105569/Online_safety_in_schools_and_colleges.Questions_from_the_Governing
_Bo ard__2022_.pdf

This review will be carried out by the Online Safety Group whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (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 relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

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)
Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and   child protection (including online safety and understanding the filtering and monitoring   systems and processes in place). This should be explicit in the role holder's job description."*

> They (the DSL) *"are able to understand the unique 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 at school or college"*

> They (the DSL) *"*can recognise the additional risks that children with special educational   needs and disabilities (SEND) face online, for example, from bullying, grooming and   radicalisation and are confident they have the capability to

support children with SEND to stay safe online"

The DSL will:

● hold the lead responsibility for online safety, within their safeguarding role. ● 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 online safety 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 headteacher/senior leadership team

● 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)

Online Safety Lead

The Online Safety Lead will:

● lead the Online Safety Group

● work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), ● receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments

● have a leading role in establishing and reviewing the school online safety policies/documents

● promote an awareness of and commitment to online safety education / awareness raising across the school and beyond

● liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

● ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

● provide (or identify sources of) training and advice for staff/governors/parents/carers/learners

● liaise with (school/local authority/MAT/external provider) technical staff, pastoral

staff and support staff (as relevant)

- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particuarly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    -content
    -contact
    -conduct
    -commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:
- a discrete programme
- PHSE and SRE 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.

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 (AUA)
- they immediately report any suspected misuse or problem to ***Gary Jones (DSL) or Martin Borrott (OSL)*** 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 *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the SWGfL Safe Remote Learning Resource)
- 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.

IT Provider

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:
- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- 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 / MAT or other relevant body
- 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 Rachael Hatch or Martin Borrott 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 **LINKS FROM RM:**

- User-friendly safeguarding to protect your whole school'
  https://mail.google.com/mail/u/0/#search/dns/FMfcgzGqRGbwGmwVhCrCTgzDG Zkc Mgzm?projector=1&messagePartId=0.1
-     RM   Connectivity   Services   document https://mail.google.com/mail/u/0/#search/dns/FMfcgzGqRGbwGmwVhCrCTgzDG Zkc Mgzm?projector=1&messagePartId=0.2
- Safetynet Help Guides- http://rmsafetynet.helpdocsonline.com/support

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 these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement ● publish 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 AUA before being provided with access to school systems.

Online Safety Group

The Online Safety Group has the following members:
- Designated Safeguarding Lead
- Online Safety Lead
- Online Safety governor
- Technical staff
- Teacher and support staff members
- Learners
- Parents/carers

Members of the Online Safety Group will assist the DSL/OSL with:
- the production/review/monitoring of the school Online Safety Policy/documents ● the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible ● encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self review tool.

An Online Safety Group terms of reference template can be found in the appendices.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:
- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements ● is made available to staff at induction and through normal communication channels ● is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

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

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

● peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: ● Child sexual abuse imagery* ● Child sexual abuse/exploitation/grooming ● Terrorism ● Encouraging or assisting suicide ● Offences relating to sexual images i.e., revenge and extreme pornography ● Incitement to and threats of violence ● Hate crime ● Public order offences - harassment and stalking ● Drug-related offences ● Weapons / firearms offences ● Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	● Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) ● Gaining unauthorised access to school networks, data and files, through the use of computers/devices ● Creating or propagating computer viruses or other harmful files ● Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) ● Disable/Impair/Disrupt network functionality through the use of computers/devices ● Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					**X**
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online shopping/commerce X			X		X		X	
File sharing X X	X			X	X			
Social media				X	X			
Messaging/chat	X				X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok X X	X X		X		X			
Mobile phones may be brought to school X XX X X	X						X	
Use of mobile phones for learning at school	X				X			

Use of mobile phones in social time at school X	X				X			

Taking photos on mobile phones/cameras X X	Xxx X				X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi X	X				X			
Use of school e-mail for personal e-mails	X				X			

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

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, Online Safety Lead and other responsible staff 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 (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the **Computer Misuse Act**
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, 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 using the following procedures:
    - one or more senior members of staff should be involved in this process.

This is vital to protect individuals if accusations are subsequently reported. ● conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority / MAT (as relevant)
  - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on MyConcern
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to: ● *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant*

  - The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident Flowchart

Unsuitable materials or activity

Illegal materials or activities found or suspected.

Report to the Designated Safeguarding Lead

(DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them

evidence.

Secure and preserve

Debrief on online safety incident.

Record details in incident log

material is confirmed,

Review polices and share experiences

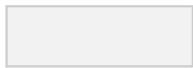Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

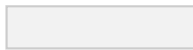and practice as required.

Await Police response.

If illegal activity or materials are confirmed, allow

Implement

changes.

If no illegal activity or
The DSL/Headteacher is responsible for

wellbeing

Police or relevant authority to complete their investigation and seek advice from the relevant

Monitor situation.

then revert to internal procedures.

the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to OSL/Assistant Headteacher	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X	X	X	X		
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords		X	X		X	X	X	X	
Corrupting or destroying the data of other users.		X	X		X	X	X	X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X		X
Unauthorised downloading or uploading of files or use of file sharing.		X	X		X	X	X	X	
Using proxy sites or other means to subvert the school's filtering system.		X	X		X	X	X	X	

Incidents								
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X						X	
Unauthorised use of digital devices (including taking images)	X	X	X			X		X	
Unauthorised use of online services	X	X	X		X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X		X	X	X	X	X

Responding to Staff Actions

Incidents	Refer to OSL	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate	**X**	**X**	**X**	**X**	X		X	X

activities)								
Deliberate actions to breach data protection or network security rules.	X	X			X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X				X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X			X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X		X			X
Unauthorised downloading or uploading of files or file sharing	X	X			X	X		
Breaching copyright or licensing regulations.	X					X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X			X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	X						
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X				X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X							
Actions which could compromise the staff member's professional	X	X						

standing								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X			X			
Failing to report incidents whether caused by deliberate or accidental actions	X	X				X		
Continued infringements of the above, following previous warnings or sanctions.	X	X					X	X

Online Safety Education Programme

Keeping Children Safe in Education states:

> "*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum ...*"

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- 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**.** This is evident in Knowledge Organisers.
- 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.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be 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
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

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.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors* ● *the Online Safety Group has learner representation*

- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- *the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Designated Safeguarding Lead/Online Safety Lead will provide advice/guidance/training to individuals as required.*

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:
- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to undestand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

The school will seek to provide information and awareness to parents and carers through: ● *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*

- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers*
- *Sharing good practice with other schools in clusters or the local*

authority Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and   procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the   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 will have lead responsibility for   safeguarding and online safety and the IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the   Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change
  in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering.

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools 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 Appropriate filtering.
- 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.
- *the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle* ● *the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *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.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

Monitoring

 The school has monitoring systems in place to protect the school, systems and users: ● 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.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#)guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

  - physical monitoring (adult supervision in the classroom)
  - internet use is logged, regularly monitored and reviewed
  - filtering logs are regularly analysed and breaches are reported to senior leaders ● *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
  - *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
  - *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

The school technical systems will be managed in ways that ensure that 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 the SLT/Online Safety Group
- password policy and procedures are implemented.
- the security of their username and password and must not allow other users to access the systems using their log on details.
- 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. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords. ● 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 in place 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,
- DNS is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied. ● an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- 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 the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider

● 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
● guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.
The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authori se d device[2]	Stude nt owne d	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes			
Internet only						
No network access					Yes	Yes

School owned/provided devices:
> ● *all school devices are managed though the use of Mobile Device Management software*
> ● *there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed*
> ● *any designated mobile-free zone is clearly signposted*
> ● *personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.*
> ● *the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.*
> ● *liability for damage aligns with current school policy for the replacement of*

equipment.
- *education is in place to support responsible use.*

Personal devices:
- *there is a clear policy covering the use of personal mobile devices on school premises for all users*
- *where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.*
- *where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.*
- *use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems*

[2] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- *the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.*
- *liability for loss/damage or malfunction of personal devices is clearly defined* • *there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes*

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:
- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions. • risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:
- No reference should be made in social media to learners, parents/carers or school staff.

- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be: ● a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken ● *the school permits reasonable and appropriate access to personal social media sites during school hours*

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. ● staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites,
  nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- *staff and volunteers are allowed to take digital/video images **on school devices** to support   educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images*
- *care should be taken when sharing digital/video images that learners are appropriately dressed*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy*
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy ● *learners'*

work can only be published with the permission of the learner and parents/carers.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:
- ● Public-facing website
- ● Social media (Facebook, Instagram, Class Dojo)
- ● Online newsletters

The school website is managed/hosted by e4education. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.
The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:
- ● has a Data Protection Policy.
- ● implements the data protection principles and can demonstrate that it does
so ● has paid the appropriate fee to the Information Commissioner's Office
(ICO) ● has appointed an appropriate Data Protection Officer (DPO) who has effective
    understanding of data protection law and is free from any conflict of interest. ●
has a 'Record of Processing Activities' in place and knows exactly what personal data is

held, where, why and which member of staff has responsibility for managing it ● the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed

● 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

● provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice

● has procedures in place to deal with the individual rights of the data subject
● carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier

● 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

● has a Freedom of Information Policy which sets out how it will deal with FOI requests ● 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: ● data will be encrypted, and password protected.
 ● 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.

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.