St Margaret’s CE Junior School

Online Safety Policy

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).

Adopted as draft (Consultation): 1st September 2025

Agreed by Governors (signatures on Governor Hub): 9th October 2025

Next review date: October 2026

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St Margaret's CE Junior 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, 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).

The 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.

The 4 Cs

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: 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, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Policy development, monitoring and review

This Online Safety Policy has been developed by

- Headteacher
- Online safety lead
- Staff – including teachers/support staff/technical staff
- Pupil Online Safety Leaders
- Member of the governing body

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:*	*9th October 2025*
The implementation of this Online Safety Policy will be monitored by:	*DSL / 'Online Safety Lead' / 'Online Safety Governor"*
Monitoring of policy:	*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:	*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:	*October 2026*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Staffordshire Children's Advice & Support team / Police*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- surveys/questionnaires of:
  - learners
  - parents and carers
  - 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[1] 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 may be delegated to the Online Safety Lead.
- 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[2].
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, 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 Online Safety Lead.

Governors

- Governors are responsible for the approval of the Online Safety Policy. They will ensure 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.

- Online safety, including filtering and monitoring and cyber-security are discussed during governing board meetings.

Governors should take part in online safety training/awareness sessions, with particular importance for the link governors involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- participating in relevant training such as online safety
- participation in school training / information sessions for staff or parents (this may include attendance at worship/lessons)

Designated Safeguarding Lead (DSL)

The designated safeguarding lead takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues:

- sharing of personal data [3]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying
- radicalisation
- additional risks that children with SEND face online, including those above

[3] See 'Personal data policy' in the Appendix.

The Designated Safeguarding Lead and the Online Safety Lead work closely in collaboration because online safety issues often relate to safeguarding.

All online safety incidents are recorded by the online safety lead and shared with the DSL/Headteacher. Further action is taken where relevant, including liaising with agencies.

Online Safety Lead

The Online Safety Lead will:

- work with pupil digital leaders
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined, reporting to governors where relevant
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- 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
- receive reports of online safety incidents[4] and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- report to governors, minimum annually, to discuss current issues, review incidents and update the filtering and monitoring logs
- report regularly to headteacher/senior leadership team.

Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme
- PSRHE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities

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 follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements
- they immediately report any suspected misuse or problem to the headteacher/online safety lead for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be 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 and implement current policies regarding these devices
- in lessons where internet use is pre-planned 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- have 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
- they adhere to the school's policies, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated

IT Provider / technical staff

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

The IT Provider/technical staff (Staffs Tech) is responsible for ensuring that:

- they are aware of and follow the school Online Safety 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 local authority 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 Online Safety Lead/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 software/systems are implemented and regularly updated as agreed in school policies

The IT service provider works with the senior leadership team and DSL to procure systems, identify risks and carry out reviews.

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety
- 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.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

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
- 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.

Online Safety Group

The Online Safety Group has the following members

- Online Safety Lead
- Designated Safeguarding Lead
- senior leaders
- online safety governor
- technical staff
- learners

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy (IWF Compliant) 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
- pupils are encouraged to share their knowledge with staff to raise awareness of emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- 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

Online safety and the school approach to it is reflected in the child protection 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

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 launderingc					X
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)					X
Users shall not undertake	Accessing inappropriate material/activities online in a school setting including pornography,				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
activities that are not illegal but are classed as unacceptable in school policies:	gambling, drugs. (Informed by the school’s filtering practices and/or AUAs)					
	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 or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				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/awaren
Online gaming	X				X			

Online shopping/commerce			X		X			
File sharing			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
Mobile phones may be brought to school (Pupil phones kept locked away by staff / staff use only when no pupils present)			X					X
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras	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			
Use of school e-mail for personal e-mails	X				X			
Use of AI services that have not been approved by the school	X				X			

When using communication technology, 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 and the Staff Code of Conduct 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

Reporting and responding

School and college leaders create a culture where sexual harassment and online sexual abuse are not tolerated. Should any issues arise we intervene early to better protect children and young people. We make the assumption that sexual harassment and online sexual abuse is happening in our community, even when there are no specific reports.

Our child-on-child abuse policy sets out our approach, including routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse.

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:

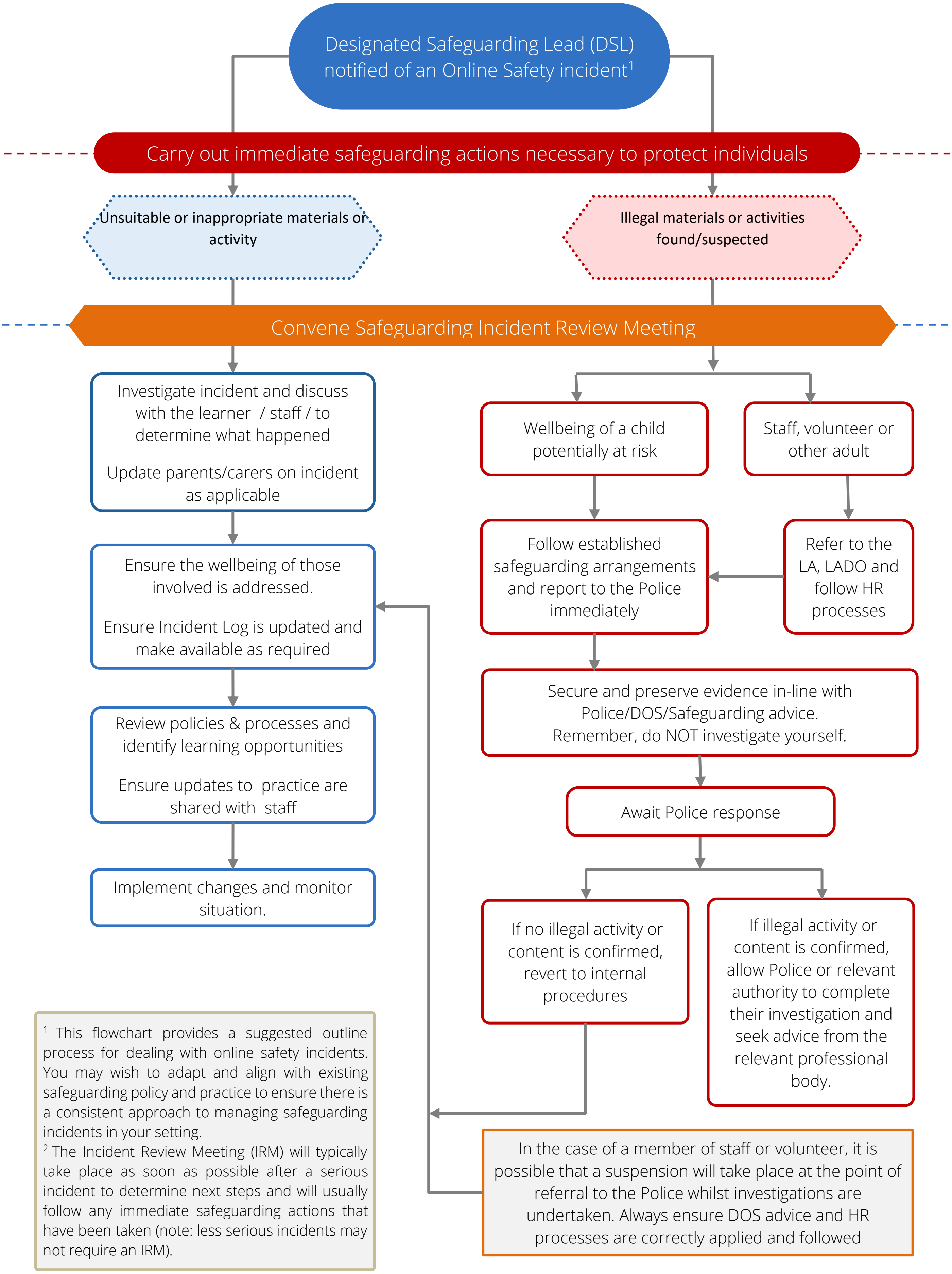
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware 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, 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, procedures or sanctions
    - involvement by local authority
    - 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
- 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 discussed (and followed up) by the DSL and Online Safety Lead

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



Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated and make available as required

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA, LADO and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.

Await Police response

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

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 Head of Department / Principal Teacher / Deputy Head	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	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list on unsuitable/inappropriate activities).	X	X	X	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	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			
Unauthorised downloading or uploading of files or use of file sharing.	X	X				X	X		
Using proxy sites or other means to subvert the school's filtering system.		X	X			X	X		X

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
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
Unauthorised use of online services		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
Continued infringements of the above, following previous warnings or sanctions.		X	X			X	X		X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	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 activities)		X	X	X	X		X	X
Actions to breach data protection or network / cybersecurity rules.		X			X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	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
Using proxy sites or other means to subvert the school's filtering system.		X			X			X
Unauthorised downloading or uploading of files or file sharing	X	X				X		X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	X	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		X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X	X			X		X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X				X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X				X		
Actions which could compromise the staff member's professional standing		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
Failing to report incidents whether caused by deliberate or accidental actions	X	X				X		X
Continued infringements of the above, following previous warnings or sanctions.		X	X					X

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in , its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks (including how to engage responsibly), and ethical and social impacts.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.

- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will assess the AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school
- Staff should ensure that they maintain Transparency in AI-Generated Content.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

We have a whole school approach to safeguarding and related policies and procedures. This includes considering online safety whilst planning the curriculum, as stated in Keeping Children Safe in Education.

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 Education for a Connected Work Framework by UKCIS/DCMS 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
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas
- 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.
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- adaptations are made for the specific needs of individual children e.g. 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
- 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 / tools (including AI systems) the learners visit
- it is accepted that from time to time, for good educational reasons, learners 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:

- we encourage pupils to provide feedback to staff about online safety and technology
- appointment of digital leaders/various pupil groups
- the Online Safety Group includes digital leaders
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns, worships
- learners contribute to the design/updating of acceptable use agreements

Staff/volunteers

Staff receive appropriate safeguarding training, including online safety, minimum annually and at induction. In addition, staff briefings (bi-weekly) provide staff with regular safeguarding updates (including online safety). Online safety forms part of the whole school approach to safeguarding, incorporating staff training and curriculum planning.

All staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of online safety, cyber-security (and data protection) training. This is renewed annually and staff online safety training needs are audited
- 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 modelling positive online behaviours
- use of school systems, online and social media is also included in our Staff Code of Conduct

- the Online Safety Lead (OSL) and DSL (or other nominated person) keep updated through relevant CPD e.g. UKSIC / SWGfL / LA / other relevant organisations and by reviewing guidance documents released by relevant organisations
- our Online Safety Policy is discussed with staff in meetings and the OSL/DSL will provide guidance and training where needed

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 relevant training
- participation in school training / information sessions for staff or parents
- A higher level of training will be made available to the Online Safety Governor, including cyber-security and understanding filtering and monitoring

Families

Parents/carers may have a limited understanding of online safety risks and issues, including potentially harmful and inappropriate material on the internet, but play an essential role in the monitoring/regulation of their children's online behaviours.

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
- pupils are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, website
- high profile events / campaigns e.g. Safer Internet Day
- provision of information and links about online safety (see Appendix for resources)
- Potential parent workshops

Technology

We have an external IT service/technology provider (StaffsTech) who we work closely with. The provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. The provider (StaffsTech) is fully aware of the school Online Safety Policy/acceptable use agreements and school has a Data Processing Agreement in place with them. (Ref: DfE Filtering and Monitoring Standards)

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 OSL/DSL updates staff on a regular basis, including about the policies and procedures in place. Everyone is responsible for online safety and data protection.

Filtering & Monitoring

The school filtering and monitoring provision is reviewed by senior leaders, governors and the IT Service Provider (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 knowledge of the OSL/DSL 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.

Checks on the filtering and monitoring system are carried out by the IT Provider with the involvement of the OSL/DSL, and reported to a governor, particularly if a safeguarding risk is identified or there is a change in working practice or technology e.g. SWGfL Test Filtering.

Filtering

Governing bodies should make sure their school or college has appropriate filtering and monitoring systems in place. The OSL/DSL reports this annually to governors. Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- roles and responsibilities of staff and IT support are clearly defined

- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. System checks are carried out half-termly and content lists are regularly updated
- there are established and effective routes for users to report inappropriate content and these are acted upon swiftly
- there is a clear process in place to deal with requests for filtering changes
- the school has differentiated user-level filtering for staff and pupils, in limited circumstances
- filtering and monitoring systems work in tandem to identify potential breaches of the filtering policy, which are then acted upon
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.
- There are regular checks on the filtering system to check its effectiveness by the IT provider and reported to the OSL/DSL. (SWGfL Testfiltering.com can do this)
- Devices that are provided by the school have school-based filtering applied
- the school has a no mobile phone policy so there is no access to the school network
- 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

Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying.

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.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. The OSL is responsible for managing the monitoring strategy and processes

- 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 by the OSL and DSL
- Technical monitoring systems are up to date and managed well, with logs/alerts reviewed regularly and acted upon
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.
- where AI–supported monitoring is used, the purpose and scope of this is clearly communicated
- The monitoring provision is reviewed at least annually and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review is conducted by the OSL/DSL/IT provider and reported to a governor.

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. 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.
- use of monitoring software that is reviewed by the OSL/DSL

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- 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 Staffs Tech and will be reviewed, at least annually, by the OSL
- all users (adults and learners) 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. Users must immediately report any suspicion or evidence that there has been a breach of security
- password policy/procedures are implemented and consistent with national guidance

- all school networks and system are protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password
- master account passwords for the school systems are kept in a secure place (offsite)
- there are reviews and audits of the safety and security of school technical systems
- appropriate security measures are in 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 (anti-virus) software
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices – this is not allowed
- systems are in place to control and protect personal data and data is encrypted at rest or in transit
- Staffs Tech/Bursar are responsible for ensuring that all software purchased and used by the school is adequately licenced and that the latest software updates are applied
- users will report any actual/potential technical incident/security breach to OSL/DSL
- Acceptable Use Policy (AUP) details: use of school devices out of school by family members is not allowed / personal use of any device on the school network is regulated by the AUP / staff are not permitted to install software on a school-owned devices without the consent of SLT/IT provider
- mobile device security and procedures are detailed in the Staff Code of Conduct
- guest users can only access school systems based on an identified risk profile
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data
- multi-factor authentication is used for accessing sensitive data outside the network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Mobile technologies

Mobile technology devices (small number and school owned) provide limited access and are protected by encryption and filtering/monitoring. 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	Authorised device[5]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes (locked away)	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only						
No network access				Yes	Yes	Yes

Personal devices

- staff are allowed to use personal devices ONLY in free time where pupils are not present
- visitors are not allowed to use their devices where children are present and cannot use their camera to take photographs, except where specifically agreed by SLT
- staff will use their mobile phone for emergency purposes on trips/visits
- no access to networks/internet for staff/visitors
- no internet connection for personal devices

[5] 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.

- no taking/storage/use of images is allowed on personal devices
- no liability for loss/damage or malfunction as no access allowed to the network
- visitors are informed about school requirements on arrival
- misuse will be dealt with in accordance with this policy, staff Code of Conduct and staff disciplinary procedures

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
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers, school staff or the school
- 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

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 – please refer to points above and Staff Code of Conduct – staff must not make social media posts about the school
- personal communications which do not refer to or impact upon the school are outside the scope of this policy

Monitoring of public social media

- As part of active social media engagement, the school may monitor the Internet for public postings about the school
- the school may 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 contact school directly, 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 can take videos/digital images of their children at school events for their own personal use (such use in not covered by the Data Protection Act). To respect everyone's privacy/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 can take digital/video images (school devices only) to support education, but must follow policies re: sharing, storage, distribution and publication of those images
- 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

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Online newsletters

The school website is managed/hosted by contentcaretaker.co.uk. 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.

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 Privacy Notice
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- 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
- ensures that where AI services are used, data privacy is prioritised

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:

- take care of all network devices, not allowing them to be used by others and keeping them in a safe place e.g. do not leave in a vehicle, particularly on view
- 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, with permission of OSL/SLT
- will not transfer any school personal data to their own personal devices. Procedures are in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided)
- 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, so that access is protected e.g. by Bit-Locker
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices
- use Multi Factor Authentication (MFA) on all devices, as set up by Staffs Tech support

Cyber Security

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-collegesCyber incidents and attacks have significant operational and financial impacts on schools. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage

(Ref: DfE Cyber security standards for schools and colleges)

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually
- the school, (in partnership with Staffs Tech), has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup/restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on common cyber security threats e.g. phishing
- the school's education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so

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:

- information taken from the reviews/audits is used to help inform learning and 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 online safety issues where relevant
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate