



FOUNTAINS

PRIMARY SCHOOL

Always achieving our potential

Online Safety Policy

Written: September 2026

To be reviewed: September 2027

Policy Owner: Miss Hannah Knight (Computing Lead Teacher)

Ratified: Mrs Nicola Price (Headteacher) September 2026



ALWAYS ACHIEVING OUR POTENTIAL

Introduction

This **Online Safety Policy** addresses current and emerging online safety issues within a whole-school context and should be read alongside other relevant policies, including the Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy and Acceptable Use Agreements.

Ensuring that pupils use digital technologies appropriately, responsibly and safely is an essential part of the school's duty of care. Through this policy, the school aims to provide a safe and secure environment in which pupils can benefit from technology while being protected from potential harm, both within and beyond the school setting.

This policy outlines the school's approach to promoting online safety, preventing harm and responding effectively to concerns. It supports the school's statutory safeguarding responsibilities and helps ensure that all members of the school community understand their roles and responsibilities when using digital technologies.

Online safety is a shared responsibility. The school works closely with pupils, staff, parents and carers to develop the knowledge, skills and behaviours needed to use technology safely and responsibly.

This policy will be reviewed annually, or sooner if required, to reflect changes in legislation, guidance, technology or emerging online safety risks.

Legislation and guidance

This Online Safety Policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education (KCSIE)**, and should be read alongside the school's Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Agreements, Data Protection Policy and Staff Code of Conduct.

The policy also reflects the DfE's non-statutory guidance and advice, including:

- *Teaching Online Safety in Schools*;
- *Preventing and Tackling Bullying* and advice on cyberbullying for school leaders and staff;
- *Relationships Education, Relationships and Sex Education (RSE) and Health Education*;
- *Searching, Screening and Confiscation* guidance; and
- *The Prevent Duty* guidance on protecting children from radicalisation.

This policy reflects relevant legislation, including but not limited to:

- The Education Act 1996;
- The Education and Inspections Act 2006;
- The Equality Act 2010;
- The Education Act 2011;

- The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR); and
- The Online Safety Act 2023.

The school recognises its responsibility to safeguard and promote the welfare of children and young people in an increasingly digital world. Online safety is a fundamental part of safeguarding and should be viewed as a shared responsibility between pupils, staff, governors, parents and carers.

The DfE states:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."

The Governing Body will ensure that online safety remains a running and interrelated theme throughout the school's safeguarding arrangements, curriculum, staff training, policies and procedures. Online safety considerations will be embedded in all relevant aspects of school life.

Annual Review and Risk Assessment

Technology continues to evolve rapidly, creating new opportunities as well as emerging risks. The school will review its Online Safety Policy annually and undertake a regular online safety risk assessment to ensure that procedures, filtering systems, monitoring arrangements and educational approaches remain effective and appropriate to the needs of pupils.

The school may also use recognised self-review tools, such as the **360 Safe Online Safety Self-Review Tool**, to support continuous improvement in online safeguarding practice.

Online Safety Risks:

The school recognises that online safety risks are broad, continually evolving and can generally be categorised into four areas:

Content

Children may be exposed to illegal, inappropriate or harmful content, including:

- misinformation and disinformation;
- AI-generated content and deepfakes;
- extremist material;
- racist, misogynistic, homophobic or discriminatory content;
- self-harm and suicide-related content;

- 
- conspiracy theories; and
 - other harmful or age-inappropriate material.

Contact

Children may be subjected to harmful online interactions with others, including:

- online grooming;
- child sexual exploitation;
- criminal exploitation;
- peer pressure;
- coercion and manipulation;
- commercial advertising; and
- adults posing as children or young people.

Conduct

Children's own online behaviour may increase risk, including:

- cyberbullying;
- sharing personal information;
- sharing, creating or distributing inappropriate content;
- misuse of social media;
- creating or sharing AI-generated images, videos or audio;
- sharing of nude or semi-nude images; and
- behaviours that place themselves or others at risk.

Commerce

Children may be exposed to risks associated with online commercial activity, including:

- phishing;
- scams and fraud;
- in-app purchases;
- gambling;

- inappropriate advertising; and
- financial exploitation.

Curriculum and Education

The school will teach online safety through a broad and balanced curriculum, including Computing, Relationships Education and Health Education. Online safety education will be age-appropriate, relevant and responsive to emerging technologies and risks. The school will also draw upon the UK Council for Internet Safety's Education for a Connected World Framework to support pupils in developing the knowledge, skills and behaviours needed to navigate the online world safely and responsibly.

The school is committed to developing a culture in which pupils are empowered to use technology safely, respectfully, responsibly and securely, and know how to seek support if they encounter concerns online.

Scope of the Online Safety Policy

This Online Safety Policy outlines The Fountains Primary School's commitment to safeguarding and promoting the welfare of all members of the school community when using digital technologies and online services.

This policy applies to all members of the school community, including pupils, staff, governors, volunteers, parents and carers, visitors, contractors and community users who access or use the school's digital systems, both on and off site. It also applies to the use of personal digital devices on the school premises where such use is permitted.

The school recognises that online safety incidents may occur both within and beyond the school environment. Where incidents involving members of the school community are identified, the school will respond appropriately in accordance with this policy and other relevant policies, including the Behaviour Policy, Anti-Bullying Policy and Safeguarding and Child Protection Policy.

Where appropriate and proportionate, and where incidents are known to the school, parents and carers will be informed of significant online safety concerns or incidents involving their child that occur outside of school.

Policy development, monitoring and review

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

- headteacher/senior leaders **Nicola Price Headteacher, Abi Wilburn Assistant Headteacher**
- Designated safeguarding lead (DSL) **Laura Kobylanski**
- Online Safety Lead (OSL) **Abi Wilburn, Hannah Knight**
- staff – including teachers/support staff/technical staff- **Adam Livett**
- Safeguarding governors **Pam Simkin**

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 <i>school governing body</i> on:	
The implementation of this Online Safety Policy will be monitored by:	<i>Nicola Price, Abi Wilburn, Hannah Knight, Pam Simkin, Laura Kobylanski.</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>governing body</i> 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:	<i>3x Year at Governor's Meetings</i>
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:	<i>01/09/2027</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LADO, Esteem MAT, Police</i>

Process for monitoring the impact of the Online Safety Policy

The effectiveness of this policy will be monitored and reviewed regularly by the Designated Safeguarding Lead (DSL), **Laura Kobylanski**, and reported to governors where appropriate.

The impact of the policy will be evaluated through:

- Records and logs of online safety incidents and concerns;
- Filtering and monitoring reports;
- Internal monitoring data relating to network and device usage;
- Feedback gathered through surveys and questionnaires from:
 - pupils;
 - parents and carers; and
 - staff;
- Safeguarding records and reported online safety concerns;
- Feedback from governors, staff training and curriculum reviews.



This monitoring will help identify emerging risks, evaluate the effectiveness of current procedures and inform future improvements to the school's online safety provision.

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 and Senior Leadership Team are responsible for promoting a strong culture of safeguarding and ensuring that online safety is embedded throughout the school.

They will:

- Ensure that effective online safety policies, procedures and practices are in place and implemented consistently across the school.
- Recognise that, whilst overall accountability rests with the Headteacher, the day-to-day leadership of online safety is delegated to the Designated Safeguarding Lead (DSL).
- Be familiar with the procedures to be followed in the event of an online safety concern or allegation involving a member of staff.
- Ensure that the DSL, Online Safety Lead, IT service providers and other relevant staff are able to fulfil their responsibilities effectively and receive appropriate training.
- Ensure that robust filtering and monitoring systems are in place, regularly reviewed and effective in safeguarding pupils.
- Work in partnership with governors, the DSL and IT service providers to oversee filtering, monitoring and online safety arrangements.
- Establish systems to monitor the effectiveness of the school's online safety provision and to support staff responsible for monitoring online activity.
- Receive and review regular reports on online safety incidents, trends, filtering and monitoring, and any emerging risks.
- Ensure that sufficient resources are allocated to support the effective implementation of this policy.

Governors

The Governing Body recognises its statutory responsibility for safeguarding and promoting the welfare of children, including online safety. Governors will ensure that appropriate policies, procedures and systems are in place to safeguard pupils and staff when using technology and online services.

The Governing Body will:

- Approve and review the Online Safety Policy on a regular basis, ensuring it remains effective and reflects current legislation, guidance and best practice.
- Ensure that online safety is embedded within the school's wider safeguarding arrangements.
- Ensure that an appropriately trained Designated Safeguarding Lead (DSL) is appointed and that they have lead responsibility for safeguarding and child protection, including online safety.
- Provide strategic oversight of the school's online safety provision, including filtering and monitoring arrangements.
- Receive regular reports on online safety incidents, trends, emerging risks and the effectiveness of the school's online safety procedures.
- Support the school in promoting online safety awareness among pupils, staff, parents and carers.

The Governing Body will appoint a designated Safeguarding Governor who oversees the Online Safety in school, they will:

- Meet regularly with the Designated Safeguarding Lead (DSL) and, where appropriate, the Online Safety Lead.
- Receive anonymised reports relating to online safety incidents and concerns.
- Monitor the implementation of the Online Safety Policy and ensure that online safety education and staff training are taking place as planned.
- Support the annual review of the school's filtering and monitoring arrangements in line with the Department for Education's Filtering and Monitoring Standards.
- Report on online safety matters to the Governing Body.
- Act as a link governor for online safety and support the school's ongoing development in this area.

The Governing Body will also encourage parents, carers and the wider community to engage with the school's online safety initiatives and promote safe and responsible use of technology both in and beyond the school environment.

Designated Safety Lead (DSL)

Keeping Children Safe in Education (KCSIE) 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."

KCSIE also states that the DSL should:

"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."

In addition, the DSL should:

"Recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example from bullying, grooming and radicalisation, and be confident they have the capability to support children with SEND to stay safe online."



Whilst the overall responsibility for online safety sits with the Designated Safeguarding Lead and cannot be delegated, the school may appoint an Online Safety Lead or other appropriately trained staff to support the DSL in carrying out their responsibilities.

The Designated Safeguarding Lead will:

- Take lead responsibility for online safety as part of their wider safeguarding duties.
- Ensure that online safety is embedded within the school's safeguarding culture and procedures.
- Undertake regular and appropriate online safety training to maintain up-to-date knowledge of emerging technologies, risks and safeguarding concerns.
- Work closely with senior leaders, governors and IT service providers to ensure effective filtering and monitoring systems are in place and reviewed regularly.
- Meet regularly with the Safeguarding Governor who oversees the Online Safety to discuss online safety developments, incidents, filtering and monitoring arrangements, and any emerging risks.
- Contribute to relevant governor meetings and provide updates on online safety matters where required.
- Provide regular reports to the Headteacher and Senior Leadership Team.
- Receive, record and manage online safety concerns and incidents in accordance with safeguarding procedures.
- Determine when concerns should be escalated or referred to external agencies, including children's social care, the police, the Local Authority Designated Officer (LADO) or other relevant services.
- Ensure that online safety incidents are accurately recorded and monitored to identify trends and areas for improvement.
- Liaise with staff, parents, carers and external agencies on matters relating to online safety, safeguarding and pupil welfare.
- Support staff in recognising, responding to and reporting online safety concerns.
- Ensure that pupils, including those with SEND and other vulnerabilities, receive appropriate support to remain safe online.

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- Work closely with the Designated Safeguarding Lead (DSL) on all matters relating to online safety and digital safeguarding.
- Receive and coordinate reports of online safety concerns, recognising when issues may constitute a safeguarding or child protection concern and ensuring that these are recorded appropriately.
- Support the development, implementation and regular review of the school's Online Safety Policy and related procedures.
- Promote awareness of online safety and encourage a positive culture of safe and responsible technology use across the school community.
- Work with curriculum leaders to ensure that online safety education is planned, mapped, embedded and regularly evaluated throughout the curriculum.

- Ensure that all staff understand their responsibilities regarding online safety and are familiar with the procedures for reporting concerns and incidents.
- Identify, arrange or deliver appropriate online safety training, guidance and resources for staff, governors, pupils, parents and carers.
- Liaise with senior leaders, technical support providers, pastoral staff and other relevant professionals to ensure effective online safety provision.
Keep up to date with developments in technology, legislation, guidance and emerging risks through relevant training and professional development.
- Support the monitoring and evaluation of filtering and monitoring systems and online safety procedures.
- Maintain an understanding of the four areas of online risk identified in Keeping Children Safe in Education:
 - Content – exposure to harmful, illegal or inappropriate content;
 - Contact – harmful interaction with others online;
 - Conduct – unsafe or inappropriate online behaviour; and
 - Commerce – risks associated with online financial activity, scams and exploitation.

Curriculum Leads

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

Online safety education will be delivered through:

- A planned and progressive online safety programme;
- Computing lessons;
- PSHE and Relationships Education;
- A mapped cross-curricular approach that reinforces key online safety messages across subjects;
- Assemblies, pastoral support and wider safeguarding activities;
- Theme days, workshops and enrichment opportunities;
- National awareness initiatives, including **Safer Internet Day** and **Anti-Bullying Week**.

Curriculum Leads will also:

- Ensure that online safety education is appropriately planned, sequenced and embedded within the curriculum;
- Regularly review and evaluate the effectiveness of online safety teaching and learning;
- Support staff in delivering high-quality online safety education;
- Ensure that teaching reflects current and emerging online risks, including cyberbullying, misinformation and disinformation, online scams, inappropriate content, social media, gaming, artificial intelligence (AI) and the safe use of digital technologies;
- Promote pupil understanding of how to stay safe, behave responsibly and seek help when concerns arise online.

Teaching and support staff

School staff are responsible for ensuring that:

- Maintain an awareness of current online safety issues, emerging technologies and relevant trends.
- Be familiar with, and follow, the school's Online Safety Policy and related safeguarding procedures.

- Understand that online safety is a key element of safeguarding and child protection.
- Read, understand and sign the Staff Acceptable Use Agreement (AUA).
- Immediately report any online safety, safeguarding or technology-related concerns to the Designated Safeguarding Lead (DSL), **Laura Kobylanski**, in accordance with the school's safeguarding procedures.
- Ensure that all digital communication with pupils, parents and carers is professional, appropriate and conducted only through approved school systems and platforms.
- Embed online safety education within teaching and learning, where appropriate.
- Support pupils in understanding and complying with the Online Safety Policy and Acceptable Use Agreements.
- Promote good digital literacy, including safe online research, critical evaluation of information, copyright awareness and avoidance of plagiarism.
- Supervise and monitor the use of digital technologies, devices, cameras and online resources during lessons and school activities, in accordance with school policies.
- Ensure that pupils access age-appropriate online content and that procedures are followed if unsuitable material is encountered.
- Follow national and local safeguarding guidance when using video conferencing, live streaming or other forms of remote learning.
- Challenge and report incidents of cyberbullying, online abuse, sexual harassment, discrimination, hate-related behaviour or any other inappropriate online conduct.
- Model safe, responsible and professional online behaviour at all times, including when using social media and personal technology outside of school.

IT Provider

The Department for Education's Filtering and Monitoring Standards emphasise that effective filtering and monitoring arrangements require close collaboration between senior leaders, governors, the Designated Safeguarding Lead (DSL) and IT service providers.

Where technical support is provided by an external contractor, The Fountains Primary School will ensure that the provider meets the school's safeguarding requirements and complies with this Online Safety Policy, Technical Security Policy and all relevant safeguarding procedures.

The IT Service Provider is responsible for:

- Maintaining secure and effective filtering and monitoring systems in line with the Department for Education's Filtering and Monitoring Standards.
- Providing appropriate filtering and monitoring reports to the Headteacher, DSL and other authorised staff as required.
- Undertaking actions arising from filtering and monitoring concerns, system reviews or safeguarding investigations.
- Ensuring that the school's technical infrastructure is secure, reliable and protected from misuse, unauthorised access and malicious attack.
- Supporting the school in meeting the Department for Education's Digital and Technology Standards and other relevant statutory requirements.
- Maintaining clear and secure user account management processes, including appropriate access controls and permissions.
- Working with senior leaders, governors and the DSL to identify risks, review provision and implement improvements where required.

- 
- Keeping up to date with developments in technology, cyber security and online safety in order to provide effective technical support and advice.
 - Monitoring the use of school technology and reporting concerns, misuse or attempted breaches of security to the Headteacher and/or DSL in line with school procedures.
 - Ensuring that filtering systems are regularly reviewed, tested and updated to reflect emerging risks and safeguarding concerns.
 - Implementing and maintaining monitoring systems that enable the school to identify potential safeguarding issues and respond appropriately.
 - Supporting the school's annual review of filtering and monitoring arrangements and contributing to risk assessments where required.
 - Ensuring that prompt action can be taken to address identified vulnerabilities, safeguarding concerns or technical issues.

The IT Service Provider will work closely with the Headteacher, Senior Leadership Team, DSL and Safeguarding Governor to ensure that filtering and monitoring arrangements remain effective, proportionate and appropriate to the needs of the school community.

Pupils

Pupils are expected to:

- Use the school's digital technologies, devices, networks and online services responsibly and in accordance with the Pupil Acceptable Use Agreement and this Online Safety Policy.
- Treat others with respect when communicating and interacting online.
- Understand the importance of reporting any concerns, abuse, bullying, misuse of technology or access to inappropriate content to a trusted adult.
- Know how to seek help and support if they feel unsafe, worried or vulnerable when using online technologies.
- Follow the guidance and advice provided by the school on safe and responsible use of the internet and digital devices.
- Take responsibility for their own online behaviour and understand that their actions online may have consequences both within and beyond the school environment.
- Understand the importance of protecting personal information and maintaining the privacy and security of their accounts and devices.
- Apply safe online practices when using technology outside school and recognise that behaviour which impacts the safety, wellbeing or reputation of members of the school community may be addressed by the school, even when it occurs off-site.

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
- 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.

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

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members

- Designated Safeguarding Lead
- Online Safety Lead
- senior leaders
- Safeguarding Governor who oversees the Online Safety
- technical staff
- learners

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

The same high standards of professional conduct expected in all aspects of school life apply equally to the use of digital technologies and online communication.

All staff are expected to maintain professional boundaries when communicating online and to ensure that any communication with pupils, parents, carers and other members of the school community is appropriate, transparent and conducted through approved school systems and platforms.

The school will ensure that clear policies, procedures and protocols are in place for the use of digital technologies, social media, email, messaging services, video conferencing and other forms of online communication. Staff must comply with these procedures at all times and model safe, responsible and professional online behaviour.

Any breaches of professional standards relating to the use of technology or online communication will be managed in accordance with the school's safeguarding, staff conduct and disciplinary procedures.

Policy – Online Safety Policy

Keeping Children Safe in Education states that:

"Online safety and the school or college's approach to it should be reflected in the child protection policy."

The school's Online Safety Policy:

- Sets out expectations for the safe, responsible and appropriate use of digital technologies for learning, administration and communication.
- Clearly defines the roles and responsibilities of staff, governors, pupils, parents/carers and other members of the school community in supporting online safety.
- Is reviewed regularly to ensure it reflects current legislation, safeguarding requirements, emerging technologies and online safety risks.
- Provides guidance for staff on the safe and professional use of technology, helping to safeguard both themselves and pupils.
- Supports staff in understanding their role in protecting children and promoting safe online behaviours.
- Outlines how the school educates pupils to become safe, responsible and respectful users of technology and online services.
- Establishes clear procedures for identifying, reporting, recording and responding to online safety incidents and concerns, including access to external support and advice where appropriate.
- Is supported by a range of related policies, procedures and Acceptable Use Agreements.
- Is shared with all staff during induction and through ongoing training and communication.
- Is made available to parents, carers and the wider community through publication on the school's website.

- Is implemented as part of the school's wider safeguarding and child protection arrangements.

Acceptable use

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

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be regularly promoted, understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices.

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
- splash screens
- digital signage
- 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					X

User actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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					
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	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	

User actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
unacceptable in school policies:	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 gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								

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

When using digital communication technologies, the school expects all members of the school community to follow safe, respectful and professional practices.

The school considers the following to be good practice:

- Staff must only use communication platforms and technologies that have been approved and authorised by the school for professional purposes.
- All communication between staff and pupils, parents/carers and other members of the school community must be professional in tone, appropriate in content and conducted through official school systems.
- Personal email accounts, personal mobile numbers, messaging services and personal social media accounts must not be used for communication with pupils or parents/carers.
- Staff should maintain appropriate professional boundaries at all times and ensure that their use of personal social media does not compromise their professional reputation or that of the school.
- Any communication that is offensive, discriminatory, threatening, inappropriate, suspicious or constitutes bullying or harassment must be reported immediately in accordance with the



school's safeguarding and reporting procedures. Recipients should not engage with or respond to such communications.

- All online content published on behalf of the school, including website content and social media posts, must comply with relevant school policies, including safeguarding, data protection and confidentiality requirements.
- Appropriate permissions must be obtained before publishing photographs, videos or information relating to pupils.
- Only official school email addresses should be used to identify and communicate with staff and pupils in school-related online activities.
- Staff should exercise professional judgement when creating, sharing or commenting on online content and should consider the potential impact on the school community.

Reporting and responding

The school recognises the findings of Ofsted's *Review of Sexual Abuse in Schools and Colleges* and is committed to maintaining a culture in which all forms of online abuse, harassment, harmful behaviour and safeguarding concerns are taken seriously, reported appropriately and addressed promptly.

The school will take all reasonable steps to safeguard pupils and staff online. However, it recognises that online safety incidents may occur both within and beyond the school environment and may still have an impact on members of the school community.

Reporting Concerns

The school will ensure that:

- Clear reporting procedures are in place and are understood by all members of the school community.
- Reporting arrangements are consistent with the school's safeguarding, whistleblowing, complaints and staff allegations procedures.
- Pupils, staff, parents and carers are aware of how to report online safety concerns.
- All concerns are treated seriously and responded to as quickly as possible.
- The Designated Safeguarding Lead (DSL), Online Safety Lead and relevant staff receive appropriate training to manage online safety incidents effectively.

Responding to Concerns

Any online safety concern will be risk assessed and managed in accordance with the school's safeguarding procedures.

Where there is reason to believe that an incident may involve illegal activity, criminal behaviour or a significant safeguarding risk, the matter will be escalated immediately to the Designated Safeguarding Lead and, where appropriate, external agencies.

This may include incidents involving:

- Child Sexual Abuse Material (CSAM);

- 
- Child sexual exploitation or online grooming;
 - Sharing of nude or semi-nude images;
 - Non-consensual image sharing;
 - Extremism or radicalisation;
 - Hate crime or discriminatory abuse;
 - Harassment, stalking or coercive behaviour;
 - Fraud, extortion or online scams;
 - Extreme pornography;
 - Sale or distribution of illegal substances or materials;
 - Cybercrime, hacking or offences under the Computer Misuse Act;
 - Copyright infringement or online piracy.

Where required, referrals may be made to Children's Social Care, the Police, the Local Authority Designated Officer (LADO), the Local Authority, the Multi-Academy Trust (where applicable), or other relevant agencies.

Staff Concerns

Any concern regarding the misuse of technology by a member of staff will be reported immediately to the Headteacher.

If the concern relates to the Headteacher, it will be reported directly to the Chair of Governors and, where appropriate, the Local Authority, Multi-Academy Trust or Local Authority Designated Officer (LADO).

Investigation of Incidents

Where there is no indication of illegal activity, the school may investigate concerns in accordance with its safeguarding, searching and monitoring procedures.

Any review of devices or online activity will:

- Be carried out by authorised members of staff;
- Be proportionate and lawful;
- Be appropriately documented;
- Protect the rights and welfare of all individuals involved;
- Be undertaken in line with the school's safeguarding, data protection and searching procedures.

Where concerns are substantiated, appropriate action may include:

- Educational interventions;
- Support for those affected;

-
- Application of school behaviour procedures;
 - Internal disciplinary action;
 - Referral to external agencies;
 - Police involvement where necessary.

Recording and Monitoring

The school will:

- Record all online safety concerns, incidents and actions taken using **MyConcern and/or Integris**.
- Monitor incidents to identify patterns, trends and emerging risks.
- Retain records in accordance with safeguarding and data protection requirements.
- Review incidents regularly to inform future policy, practice and curriculum development.

Support and Follow-Up

The school recognises the importance of supporting those affected by online safety incidents.

The school will:

- Provide appropriate support for pupils, staff and families affected by online safety concerns.
- Keep those who report concerns informed, where appropriate and possible.
- Inform parents and carers of significant incidents involving their child.
- Signpost individuals to external sources of advice and support where required.

Learning from Incidents

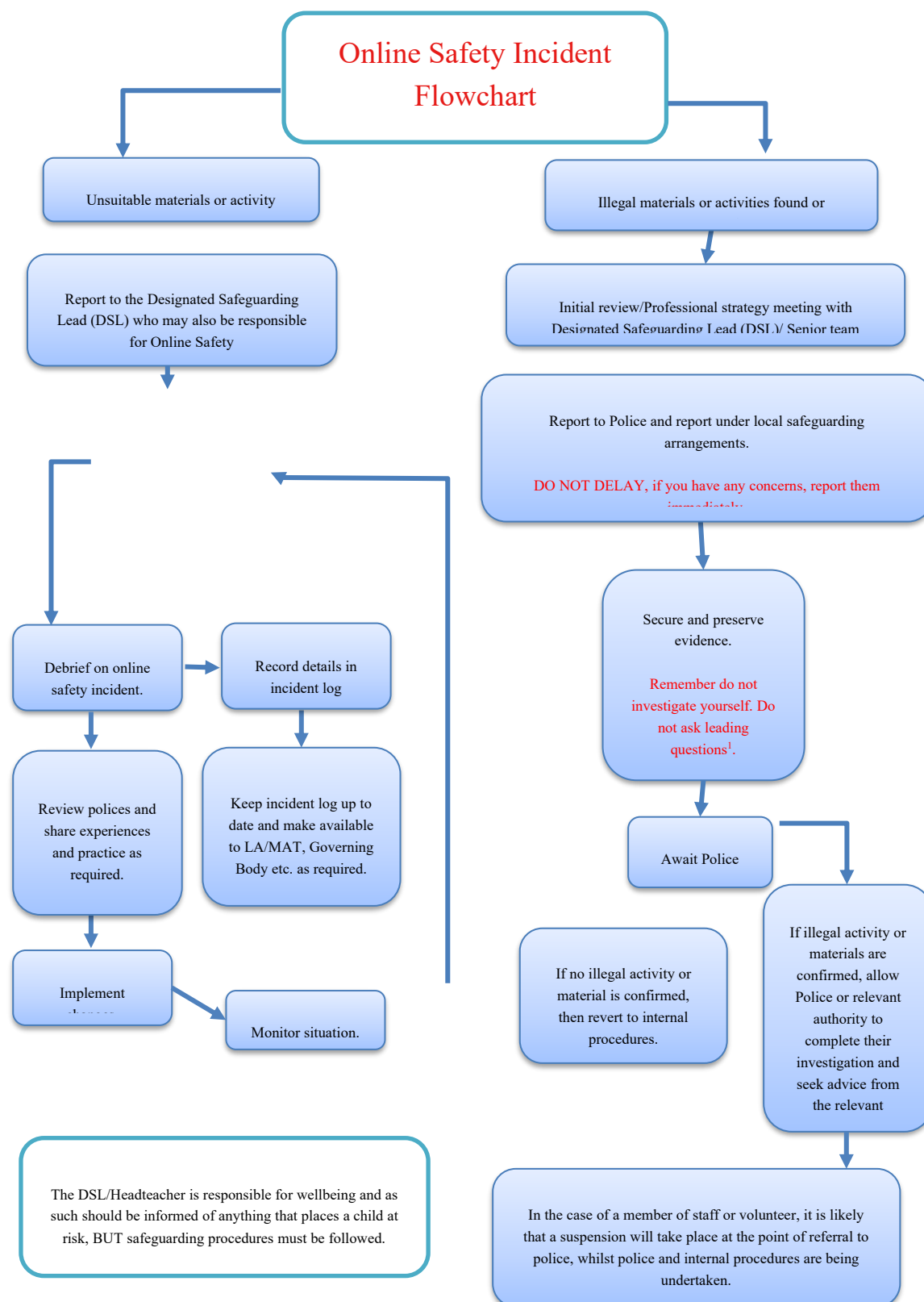
Online safety incidents will be reviewed to identify lessons learned and opportunities for improvement.

Where appropriate, anonymised information will be used to:

- Inform updates to school policies and procedures;
- Enhance staff training and awareness;
- Strengthen online safety education for pupils;
- Support communication with parents and carers;
- Inform safeguarding reports to governors.

The school will work closely with the Local Safeguarding Partnership and other relevant agencies to ensure that appropriate support is available for children who are affected by, or involved in, harmful online behaviour.

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



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/DSL	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					
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								
Corrupting or destroying the data of other users.	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								
Using proxy sites or other means to subvert the school's filtering system.	X	X	X						



Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X			X			X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X			X			X
Unauthorised use of digital devices (including taking images)	X								X
Unauthorised use of online services	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
Deliberate actions to breach data protection or network security rules.		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
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					
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					
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	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	X	X					X
Actions which could compromise the staff member's professional standing	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
Failing to report incidents whether caused by deliberate or accidental actions	X	X						
Continued infringements of the above, following previous warnings or sanctions.	X	X	X					X

Online Safety Education Programme

The Fountains Primary School delivers a planned and progressive online safety curriculum using **ProjectEVOLVE**, mapped against the UK Council for Internet Safety's **Education for a Connected World Framework**.

The online safety curriculum:

- Is taught through discrete online safety lessons and wider curriculum opportunities.
- Is age-appropriate, progressive and builds upon prior learning.
- Reflects the needs, experiences and vulnerabilities of pupils.
- Includes clear learning objectives and measurable outcomes.
- Is regularly reviewed and updated to reflect emerging technologies, trends and safeguarding risks.
- Supports pupils to develop safe, respectful and responsible online behaviours.
- Promotes digital resilience and critical thinking skills.

Areas of Learning

Through the online safety curriculum, pupils will learn about:

- Safe and responsible use of the internet and digital technologies.
- Online relationships and respectful behaviour.
- Privacy, personal information and digital footprints.
- Cyberbullying and how to seek support.
- Misinformation, disinformation and fake news.
- Online scams, phishing and commercial risks.
- Gaming, social media and live-streaming platforms.
- The safe and appropriate use of Artificial Intelligence (AI) tools.
- Online reputation and digital citizenship.
- Reporting concerns and accessing help and support.
- Age-appropriate understanding of consent, healthy relationships and online sexual harassment.

Inclusion and Accessibility



The online safety curriculum is designed to be accessible to all pupils, including those with Special Educational Needs and Disabilities (SEND), English as an Additional Language (EAL), and other identified vulnerabilities.

Where appropriate, a personalised approach will be adopted to address specific risks and support the individual needs of pupils, including those who may be more vulnerable to online harm.

Promoting Safe Online Behaviour

The school will:

- Support pupils in understanding and following the Pupil Acceptable Use Agreement.
- Reinforce online safety messages across the curriculum and wider school life.
- Provide opportunities for pupils to discuss ethical, moral and legal aspects of technology use.
- Promote understanding of relevant legislation, including the Computer Misuse Act 1990, in an age-appropriate manner.
- Encourage pupils to report concerns, worries or incidents promptly to a trusted adult.
- Participate in national initiatives such as **Safer Internet Day** and **Anti-Bullying Week**.

Safe Use of the Internet in School

Staff will:

- Model safe, responsible and professional use of technology at all times.
- Direct pupils to age-appropriate and suitable online resources wherever possible.
- Supervise and monitor internet use appropriately during lessons and school activities.
- Follow school procedures if pupils encounter inappropriate material online.
- Ensure that any temporary changes to filtering arrangements for educational purposes are authorised, risk assessed and appropriately recorded.

The effectiveness of the online safety education programme will be reviewed regularly to ensure it remains relevant, responsive and effective in meeting the needs of pupils and the wider school community.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass learner feedback and opinion. Through the Online Safety Committee.*
- *the Online Safety Group has learner representation*

- *learners contribute to the online safety education programme e.g. peer education, digital leaders, online safety campaigns*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

Keeping Children Safe in Education states:

"All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated."

The school is committed to ensuring that all staff and volunteers receive appropriate online safety training, enabling them to safeguard pupils effectively and fulfil their responsibilities under this policy.

Training and Professional Development

The school will ensure that:

- All staff and volunteers receive appropriate online safety training as part of their induction programme.
- Online safety training is integrated within the school's wider safeguarding and child protection training programme.
- Staff receive regular updates on online safety issues, emerging technologies, safeguarding risks and relevant legislation through training, briefings, staff meetings and other professional development opportunities.
- Training includes guidance on professional conduct, appropriate use of technology, online reputation, social media, classroom management and modelling positive online behaviours.
- Staff understand the school's Online Safety Policy, safeguarding procedures and Acceptable Use Agreements.
- Online safety training needs are reviewed regularly to ensure that training remains relevant and effective.
- The Designated Safeguarding Lead (DSL), Online Safety Lead and other relevant staff undertake additional specialist training and maintain up-to-date knowledge of developments in online safety, filtering and monitoring, safeguarding guidance and digital technologies.
- Updates to this policy and related procedures are shared with staff and discussed through staff meetings, training sessions and INSET activities as appropriate.
- The DSL, Online Safety Lead or other designated members of staff provide advice, guidance and support to colleagues on online safety matters when required.

The school recognises that online safety is an integral part of safeguarding. All staff and volunteers are expected to maintain up-to-date knowledge of online safety risks and contribute to creating a safe, respectful and responsible digital environment for all pupils.

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
- 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 the Safeguarding Governor who oversees the Online Safety.

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

Families and Parents/Carers

Parents and carers play a vital role in helping children stay safe online. The school recognises that families may have differing levels of confidence and understanding regarding online technologies, social media, gaming, artificial intelligence (AI) and emerging online risks.

The school will support parents and carers by:

- providing regular communication and guidance on online safety, emerging risks and reporting concerns
- offering opportunities for engagement through workshops, information sessions and regular updates via. WEDUC
- supporting parents to understand parental controls, privacy settings and age-appropriate technology use
- encouraging pupils to share online safety learning with their families
- sharing information through newsletters, the school website and other communication channels
- promoting national initiatives such as **Safer Internet Day**
- signposting families to trusted resources, including:
 - UK Safer Internet Centre (www.saferinternet.org.uk)
 - Childnet (www.childnet.com/parents-and-carers)
 - SWGfL (www.swgfl.org.uk)
 - Internet Matters (www.internetmatters.org)
 - NSPCC Online Safety Hub (www.nspcc.org.uk)
 - CEOP (www.ceopeducation.co.uk)
- working with other schools, the Local Authority and safeguarding partners to share best practice

Adults and Agencies

The school will work with families, community groups and partner agencies to promote safe and responsible use of technology. Support may be provided through:

- sharing online safety information and safeguarding messages with parents, carers and the wider community
- providing guidance and learning opportunities on the use of digital technologies, online safety and emerging online risks
- signposting the wider community to online safety resources through the school website and communication channels

- working with external agencies, safeguarding partners and community groups to promote good practice and support online safety awareness
- participating in local and national online safety initiatives and campaigns

Technology

The DfE Filtering and Monitoring Standards states that “Your IT service provider may be a staff technician or an external service provider”. If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. The school should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

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 Department for Education (DfE) requires schools to have appropriate filtering and monitoring systems in place to safeguard children online. Governing bodies and proprietors should do all that they reasonably can to limit children's exposure to harmful content and regularly review the effectiveness of their filtering and monitoring arrangements. Senior leaders, safeguarding staff and relevant technical staff should understand the systems in place, manage them effectively and ensure concerns are identified, escalated and acted upon appropriately. Filtering and monitoring arrangements should be informed by the school's safeguarding and risk assessment processes, including the Prevent Duty, and reviewed in response to emerging technologies and online risks.

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, emerging online risks, including AI technologies, and patterns of online safety incidents or behaviours.

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.

Filtering and monitoring arrangements will be reviewed in response to emerging technologies, including artificial intelligence (AI) tools and services.

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 school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre 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 (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *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 operates appropriate monitoring systems across its network, 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 (these may be outlined in the MAT).

- 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.
- 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,
- The SLT 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 (Referral form and Confide reporting system).
- 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 (where mobile devices are allowed access to school systems).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile Technologies

The school recognises that many children have access to the internet through mobile and smart technology devices, including smartphones, tablets and wearable technology. Such access may expose children to online risks including bullying, harassment, harmful content, inappropriate contact and misuse of technology. The school will manage the use of mobile and smart technology in accordance with its safeguarding, behaviour, child protection and online safety policies.

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

Teaching about the safe and appropriate use of mobile technologies, social media, artificial intelligence (AI) tools and emerging technologies is an integral part of the school's online safety curriculum.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

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 ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	Yes	Yes

School owned/provided devices

- all school devices are managed through Mobile Device Management (MDM) software and appropriate security controls, including regular updates and device management.
- 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 (Parago asset management)
- any designated mobile-free zone is clearly signposted
- the use of devices on trips/events away from school is clearly defined and expectations are clearly 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 personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
- the expectations for taking, storing and sharing images/video align with the school's Acceptable Use Policy and Use of Images 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
- personal devices must not be used to access, create, store or share inappropriate, harmful or illegal content
- 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 includes awareness of misinformation, disinformation, deepfakes, AI-generated content and online scams.
- 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
- access to personal social media during working hours is restricted and must not interfere with professional responsibilities.

Monitoring of public social media personal use

- 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.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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 is 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 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 will be taught how to identify and respond appropriately to manipulated, edited and AI-generated images and videos.
- 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
- Online newsletters
- Reach More Parents app
-

The school website is managed/hosted by Daniel Richins. 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/MAT:

- 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 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 (see Privacy Notice section in the appendix)
- 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. Procedures should be 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
- 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 of online safety incidents, safeguarding records, behaviour and bullying reports, filtering and monitoring data, and feedback from staff, pupils and parents/carers.

- evidence from reviews and audits informs ongoing improvements to online safety education, awareness, training and safeguarding practice
- online safety incidents, trends and outcomes are reported regularly to senior leaders and governors
- parents/carers are informed of relevant online safety themes, emerging risks and sources of support through the school's communication channels
- online safety policies, procedures and curriculum provision are reviewed and updated in response to incidents, audits, emerging technologies, including artificial intelligence (AI), and changes to national guidance
- the school works with partner schools, the Trust, Local Authority and other agencies to share effective practice and support a consistent approach to online safety
- the effectiveness of filtering and monitoring arrangements is reviewed regularly as part of the school's safeguarding and online safety processes