BOWERHAM PRIMARY & NURSERY SCHOOL

&

BABY UNIT

ONLINE SAFETY POLICY

DATE: July 2025

Review date: July 2026

Stand tall, reach high, love learning

The Bowerham School community is proud to nurture aspiration, inspire love for life-long learning and prepare children for a changing society.

At Bowerham School we:

- Ensure all children have access to a fun and engaging, ambitious and creative curriculum that widens their life experiences
- Develop confident and independent learners with motivation, curiosity and a love of learning
- Ensure all children learn about and demonstrate the British Values of: tolerance, mutual respect, individual liberty, democracy and rule of law, while respecting differences including gender, ethnicity, religion and ability.
- Nurture, develop and challenge children to be aspirational and secure within themselves in order to prepare them for their future

Within our Bowerham Baby Unit we follow all Bowerham Primary & Nursery School's policies and procedures. Any wording highlighted in blue within the policies are specific additions only applicable to our Baby Unit.

Introduction

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

> *"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"*
>
> *"Governing bodies and proprietors should ensure* ***online safety*** *is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how* ***online safety*** *is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"*

The DfE Keeping Children Safe in Education guidance also recommends:

> ***Reviewing online safety*** *… Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the* 360 safe self-review tool.

The DfE Keeping Children Safe in Education guidance suggests that:

> *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 nonconsensual 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.*

Schools in England are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

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).

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Bowerham to safeguard members of our school community online in accordance with statutory guidance and best practice.

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

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

Policy development, monitoring and review

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

- *Headteacher J Banks*
- *Designated safeguarding lead (DSL)- J Banks, T Clark, L Hemingway, S Harris, J Gallagher, K Ireland*
- *Online Safety Lead (OSL)- J Gallagher*
- *staff – U Essa*
- *governors- G Pollock*
- *community users- S keeves*

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:*	*Autumn 2025*
The implementation of this Online Safety Policy will be monitored by:	*All DSL's and the OLSL*
Monitoring will take place at regular intervals:	*Annually*
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Through the HT report each term*
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:	*July 26*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Depending on the incident;* *The police* *Safeguarding at Lancashire including MASH* *LADO* *Chair of governors*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
    - 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 is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and

[1] In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

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

receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

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

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"
>
> "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. 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)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

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

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards

- reporting to relevant governors committee - curriculum
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- membership of the school Online Safety Group

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

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*
>
> *They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"*
>
> *They (the DSL)* "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the school has also choosen to appoint an Online Safety Lead to work in support of the DSL in carrying out these responsibilities.

The DSL will:

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

- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

.

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Curriculum Leads

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

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes

- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

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

- they adhere to the school's technical security policy, 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

The DfE Filtering and Monitoring Standards says:

> *"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."*
>
> *"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."*
>
> *"The IT service provider should have technical responsibility for:*
>
> - *maintaining filtering and monitoring systems*
> - *providing filtering and monitoring reports*
> - *completing actions following concerns or checks to systems"*
>
> *"The IT service provider should work with the senior leadership team and DSL to:*
>
> - *procure systems*
> - *identify risk*
> - *carry out reviews*
> - *carry out checks"*
>
> "We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college,

or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

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

The IT Provider is responsible for ensuring that:

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

Learners

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

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

Parents and carers

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
- 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
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers
- community representatives

Members of the Online Safety Group will assist the DSL/OSL (or another relevant person) 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.

Professional Standards

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

- 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

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

> **"Online safety** and the school or college's approach to it should be 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 of teams
- *is published on the school website.*

Acceptable use

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

Acceptable use agreements

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.

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

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

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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Computer Misuse Act (1990)	• 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					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add 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/a
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		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			

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

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

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *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. Bowerham Primary and Nursery School is committed to ensuring that all pupils feel safe and supported in reporting online safety concerns. We understand that some children may feel more comfortable sharing worries anonymously. To support this, the school provides SWGfL Whisper, allowing pupils or parents to report concerns online anonymously.
- 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 / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police

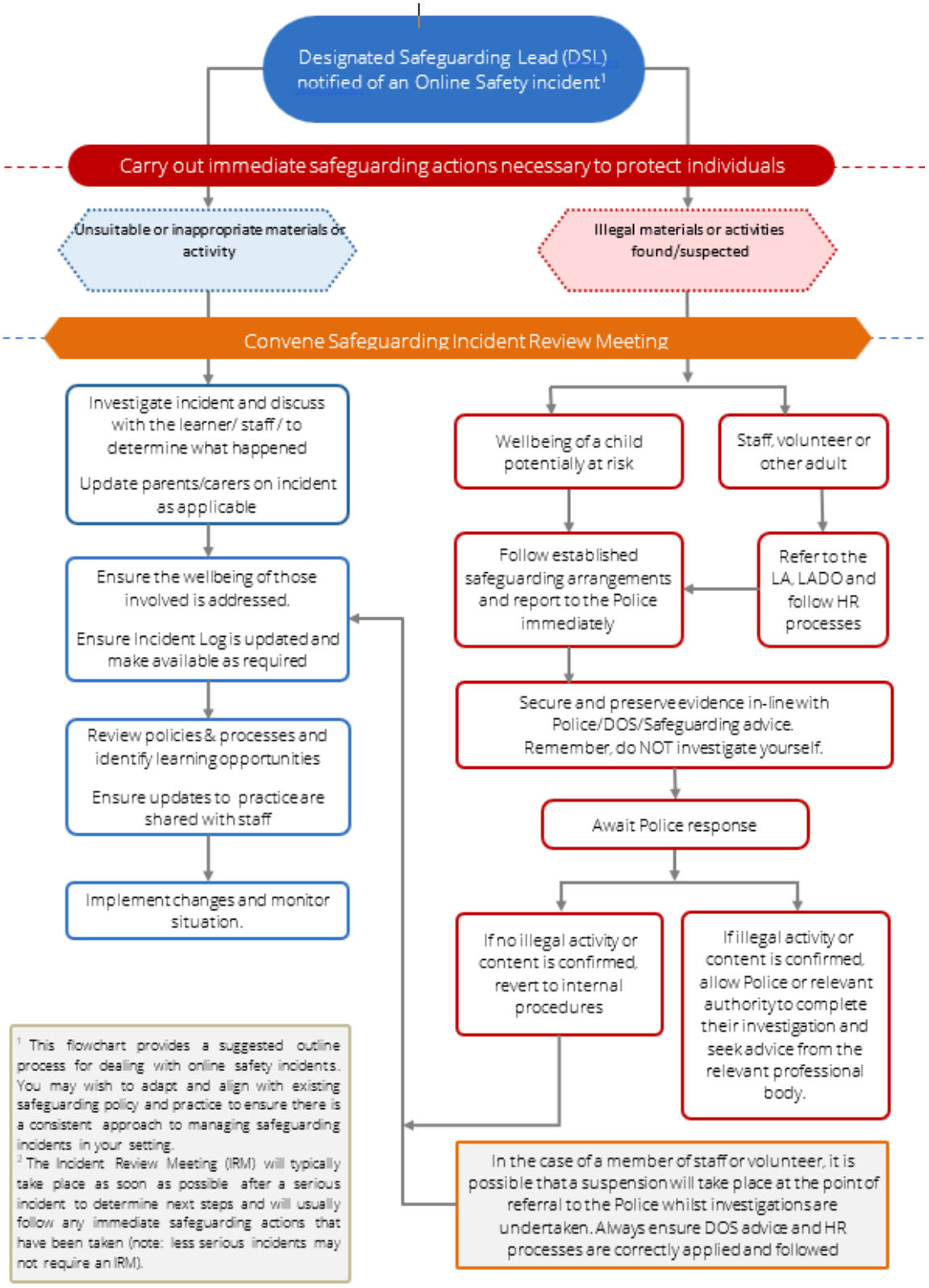
should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

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

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on an information sharing sheet immediately and shared with SLT and DSL- these will then go on CPOMS with the outcome
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings- phase meeting standing agenda*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available*

to children and young people who are victims or who perpetrate harmful sexual 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.

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

Accidentally accessing offensive or pornographic material and failing to report the incident.			X	X	X	X			
Deliberately accessing or trying to access offensive or pornographic material.			X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.			X	X	X	X	X	X	X
Unauthorised use of digital devices (including taking images)			X			X	X	X	X
Unauthorised use of online services			X					X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.			X	X	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	X	X
Actions which breach data protection or network / cyber-security rules.	X	X				X		X
Deliberate actions to breach data protection or network security rules.	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	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	X		X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files or file sharing	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations.	X	X	X	X	X	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		

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				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	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			X	X	X

The use of Artificial Intelligence (AI) systems in School

A more detailed policy can be found in the appendices, including a risk assessment matrix for the use of AI and an AI specific Staff Acceptable Use Agreement

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, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- 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.
- 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 audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- 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*
- *AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI*
- *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.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

Keeping Children Safe in Education states:

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways (statements may need to be adapted, depending on school structure and the age of the learners).

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week

- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- 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
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

As part of our commitment to preparing children for a changing digital landscape, we actively educate pupils about the responsible use of emerging technologies such as AI.

This includes:

- Helping children understand how AI tools (e.g., ChatGPT, Character.AI, Snapchat My AI) generate content, and the importance of questioning accuracy and reliability**.**

- Teaching critical thinking about misinformation, disinformation, and AI-generated bias or manipulation.
- Exploring the ethical and safeguarding concerns of using AI to create or access harmful, explicit, or inappropriate content.
- Reinforcing expectations that misuse of AI tools (e.g., sharing fake information, bullying, bypassing filters) is a serious breach of the school's Online Safety Policy**.**

These topics are woven into our PSHE, Computing, and Digital Literacy curriculum and are updated in response to national guidance and school-based trends.

Contribution of Learners

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

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

The DfE guidance "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. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

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

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

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

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

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

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers
- Sharing good practice with other schools in clusters and or the local authority/MAT

Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- *providing online safety information via their website and social media for the wider community*

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 DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

> "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…
>
> The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

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

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk

is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

Filtering

The DfE Technical Standards for Schools and Colleges states:

"Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

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

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

- a member of the SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined
- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- 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.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the

results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- 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.)
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The DfE Technical Standards for Schools and Colleges states:

"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. Monitoring solutions do not block users from seeing or doing anything."

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.

The school has monitoring systems in place to protect the school, systems and users:
- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.

- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- All children have adult supervision at all times when using devices or the internet
- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

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

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.

- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in 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 in the cloud,
- Virtue and our ICT team is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place , all staff must use the school network when in school to ensure appropriate monitoring and filtering.
- guest users are provided with appropriate access to school systems based on an identified risk profile.
- 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.

- dual-factor authentication is used for sensitive data or access outside of a trusted network

Mobile technologies

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

> *"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation.

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

The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems).

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[3]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes/No	Yes/No
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	Yes	Yes
No network access				No	No	No

School owned/provided devices:

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

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.

[3] 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.

- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge should be made available.
- use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.

- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

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

Personal use

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

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve

the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

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. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images

- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- 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

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

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

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

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

The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors

- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff
- 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:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Cyber Security

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. 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 or college 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

The School:

- 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 and review each term
- the school, (*in partnership with their technology support partner),* 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 and 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 the common cyber security threats and incidents that schools experience
- 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:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix 1

School Online Safety Policy – Artificial Intelligence in Schools

Policy on the use of Artificial Intelligence in Schools

Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

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

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI 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.

Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Staff Discipline policies and codes of conduct
- Behaviour policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements

Policy Statements

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and 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 Learners Safe
- 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 ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.
- Staff should 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.
- 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 recognize 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.
- 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*
- *AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support learners to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk*
- *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.
-

Responsibilities

Headteacher and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Online Safety Lead

Our Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and good

working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

Technical staff / IT Leads will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems. (

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

Governors/Trustees

We ensure that our governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Parents/carers

We work hard to engage parents and carers by:

- *regular in school sessions*

- *sharing newsletters*
- *sharing information online e.g., website, social media*
- *providing curriculum information*

Vulnerable groups

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- established school reporting mechanisms

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school's normal recording systems
- In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:

- Computing
- PHSE
- Cross curricular programmes

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and

evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- *Learner assessment*
- *Critical evaluation of emerging trends and research findings*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Engaging with learners*
- *Staff training*

Appendix 1a - Risk Assessment Matrix for Schools Implementing AI

Introduction

The matrix considers potential risks across various domains, including data protection, ethical considerations, and operational integrity. There is a particular focus on safeguarding and wellbeing issues, highlighting potential risks to student welfare and offers strategies to mitigate these risks effectively.

Risk Assessment Matrix

Risk Area	Risk Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (Low/Med/High)	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.	low	high	med	Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated	low	high	med	Monitor AI communication tools, implement clear

	communicatio n tools.				reporting mechanism s, and provide student support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. Reduction in teacher autonomy and critical decision-making by overusing AI tools.	low	low	low	Encourage collaborativ e learning activities and balance AI use with social engagemen t. Define clear boundaries for AI use and regularly review its impact on pedagogy.
Emotional Manipulatio n	AI systems unintentionally affecting student mental health through curated content.	low	low	low	Monitor AI-generated content, involve mental health professional s, and promote media literacy.
Inappropria te Content or Conduct	AI exposing learners to harmful or unsuitable	low	high	med	Conduct rigorous testing of AI tools, apply effective filtering and

	materials / behaviour				monitoring and ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in learners.	low	low	low	Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact student wellbeing or inclusion. AI models producing discriminatory or biased outcomes.	low	high	low	Regularly audit AI algorithms for bias and provide inclusive media literacy education and training.
Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).	low	high	low	Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-	med	med	med	Educate staff and learners to verify AI

	generated content.				outputs and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to AI tools among learners from diverse demographic groups.	low	low	low	Provide equitable access to AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of AI.	low	high	med	Provide training and education on AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	AI systems generating inaccurate or misleading recommendations.	med	high	med	Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI	low	high	low	Understand legal requirements. Conduct

	usage and learner data.				legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.	low	high	med	Strengthen cybersecurity protocols and educate staff and learners on safe online practices.

Likelihood and Impact Definitions

- **Likelihood**: The likelihood that the identified risk will occur.
    - Low: Unlikely to occur under normal circumstances.
    - Medium: Possible occurrence based on past trends or vulnerabilities.
    - High: Likely to occur without intervention.
- **Impact**: The severity of impact should the risk materialise.
    - Low: Minimal disruption with limited consequences.
    - Medium: Moderate disruption affecting key processes.
    - High: Significant disruption with severe consequences.

Appendix 1b – Staff Use of AI Acceptable Use Agreement

Artificial Intelligence (AI) and Emerging Technologies Staff (and Volunteer) Acceptable Use Agreement

School Policy

Emerging technologies, including Artificial Intelligence (AI), are increasingly integrated into educational settings and the lives of staff and learners. These technologies have immense potential to enhance creativity, promote personalized learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

- Staff and volunteers are responsible users of AI and emerging technologies, prioritising safety and ethical considerations.
- School systems and users are protected from misuse or harm resulting from the use of AI.
- Staff have a clear understanding of their responsibilities when engaging with AI and emerging technologies in professional and personal contexts.

Acceptable Use Policy Agreement

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of AI tools and technologies.
- I will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
- I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.
- I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

- I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.
- I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I will communicate professionally and responsibly when using AI systems.
- I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

- I will support learners on the safe, ethical, appropriate and effective use of AI.
- I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

- I will use AI systems in compliance with established security measures and access protocols.
- I will ensure that any AI applications used in teaching or administration comply with the school's policies.
- I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

- I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.
- I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

- I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
- I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
- I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

Appendix 2 - Staff (and Volunteer) Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g. Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems

    - will take care not to 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.
    - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
    - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- *When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses*.
- *When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.*
- *I will not use personal accounts on school systems.*
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date: