Wellington Primary School

Online Safety Policy

	Print name	Date Approved	Review Date
Headteacher	Mrs Joy Wood	July 2026	July 2027
On behalf of Governing Body	Mrs Hanna Johal		

Reporting an online safety concern (all staff)

- **Add an 'Incident'** on our Child Protection Online Management System (CPOMS).
- **Assign** it to the Designated Safeguarding Lead Joy Wood.
- **To alert** Online Safety Lead Aaron Sidebottom.

Unless the concern involves the Designated Safeguarding Lead or the Online Safety Lead, in which case the concern must be reported to:

- Chair of Governors: Mr Mark Jamieson gov.mark.jamieson@wellingtonps.co.uk
  and
- Local Authority Designated Officer (LADO): 01274 435600 / LADO@bradford.gov.uk

1. Scope of the Online Safety Policy

Our Online Safety Policy outlines the commitment of Wellington Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, pupils, volunteers, parents, guardians, carers, visitors and community users) who have access to and are users of the school's 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).

Wellington Primary School will deal with all concerns about misuse within this policy and associated policies. The school will inform parents, guardians and / or carers of incidents of inappropriate online safety behaviour that take place in school via a phone call and / or email and / or meeting. The school will inform parents, guardians and / or carers of incidents of inappropriate online safety behaviour that take place out of school via a phone call and / or email and / or meeting. This is then followed up by a letter (see appendix for proforma).

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm than others.
- Deliver an effective approach to online safety which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Our approach to online safety is based on addressing the following 4 categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as but not limited to pornography, fake news, racism, misogyny, self-harm, antisemitism, radicalization and extremism.
- Contact – being subject to harmful online interaction with other users, such as peer-to-peer pressure, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and cyber-bullying.
- Commerce – risks such as but not limited to online gambling, inappropriate advertising, phishing and / or financial scams.

The school's 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 Online Safety 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 (AUA).

- Is made available to staff at induction and through normal communication channels.
- Is published on the school's website.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education (KCSiE) September 2025, and its advice on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.
- Relationships and health education.
- Searching, screening and confiscation.

It also refers to the DfE's guidance on Protecting Children from Radicalization and Meeting Digital and Technological Standards in Schools and Colleges. It reflects existing legislation, including but not limited to: the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is 'good reason' to do so. This policy also considers the National Curriculum computing programmes of study.

4. Development, monitoring and review

This Online Safety Policy has been developed by the Computing Curriculum Lead, the Headteacher / Designated Safeguarding Lead (DSL), Online Safety Lead, Senior Leaders and Governors. The school will monitor the impact of the policy by:

- Regularly reviewing logs of reported incidents from our filtering and monitoring reports of internet activity (including sites visited).
- Regularly reviewing relevant Child Protection Online Management System (CPOMS) reports.

This Online Safety Policy was developed by:	V1: Mrs Cochrane (Computing Curriculum Lead) V2: Mr Sidebottom (Deputy Head Teacher and Online Safety Lead) V3: Mr Sidebottom (Deputy Head Teacher and Online Safety Lead) V4: Mr Sidebottom (Deputy Head Teacher and Online Safety Lead)
This Online Safety Policy was approved by the school governing body on:	V1: 17/07/2023 V2: July 2024 V3: July 2025 V4: July 2026

The implementation of this Online Safety Policy will be monitored by:	Mrs Wood (Head Teacher and Designated Safeguarding Lead) Mr Sidebottom (Deputy Head Teacher and Online Safety Lead) Mrs Berry (Assistant Head Teacher) Mark Jamieson (Chair of Governors)
The Governing Body will receive a report of anonymized details of online safety incidents from our internet filtering and monitoring logs, generated by the Online Safety Lead. They will review incidents and discuss current issues.	During the standing "Safeguarding" agenda item in full Governing Body Meetings, 6 Times / Year (every half term).
Governor monitoring of the implementation of this policy will take place at regular intervals.	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be.	July 2027
Should serious online safety incidents take place, the following external persons / agencies should be informed:	The Local Authority Designated Officer (LADO)

5. Roles and responsibilities

- Designated Safeguarding Lead (DSL) - Head Teacher - Mrs Wood
- Deputy Designated Safeguard Lead (DDSL) - Deputy Head Teacher - Mr Sidebottom
- Deputy Designated Safeguarding Lead (DDSL) - Assistant Head Teacher - Mrs Berry
- Senior Leader - Deputy Head Teacher - Mr Sidebottom
- Senior Leader - Assistant Head Teacher - Mrs Berry
- Online Safety Lead - Deputy Head Teacher - Mr Sidebottom
- Data Protection Lead - Business Manager - Mrs McMahon
- Data Protection Officer - Impero Solutions Ltd (https://www.imperosolution.com/#h.1s6mkst1tvwh)
- Computing Curriculum – Computing Curriculum Lead - Mrs Cochrane
- Supply teacher briefing of medical and SEND information - Office Manager - Mrs Ullah
- AUA and use of digital photos, videos and work permission forms – Office Manager and Online Safety Lead - Mrs Ullah and Mr Sidebottom
- Technical Support - Data Tools for Schools Ltd - Mr Byrnes (01422 410580)
- Software Licenses and Updates - Data Tools for Schools Ltd - Mr Byrnes
- Internet firewall, filtering and monitoring – Securely – Reports sent to Head Teacher Mrs Wood, Deputy Head Teacher Mr Sidebottom and Assistant Head Teacher Mrs Berry
- Anonymized reporting (half-termly) of online safety incidents – Deputy Head Teacher – Mr Sidebottom
- Checks (termly) of Securely - Business Manager - Mrs McMahon
- Checks (termly) of public social media for public postings about the school - Business Manager - Mrs McMahon

5.1 Governors' responsibilities

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

Governors will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. They will also ensure that all staff receive updates to ensure that they are provided with the relevant skills and knowledge to effectively safeguard children.

This review will be carried out by Governors, who will receive regular information about online safety incidents and monitoring reports. Governors will:

- Regularly receive (collated and anonymized) reports of online safety incidents.
- Monitor online safety logs.
- Annually check that the provision of online safety education provision is taking place as intended and report back to Governors.

Governors must ensure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. Governors will review the DfE's Meeting Digital and Technology Standards in Schools and Colleges guidance and support the school in:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

Governors will also support the school in encouraging parents, guardians and / or carers and the wider community to become engaged in online safety activities.

5.2 Head Teacher responsibilities

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout school.

5.3 Designated Safeguarding Lead (DSL) responsibilities

It is important to emphasize that online safety issues are safeguarding, not solely technical issues. Technology provides additional means for safeguarding issues to develop. The DSL:

- Has a duty of care to ensure the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
- Must be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Is responsible for ensuring that the Online Safety Lead, Senior Leaders, Technical Staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles.
- Will understand what filtering and monitoring systems and processes are in place on school devices and school networks.

- Will work with the Network Manager to make sure appropriate systems and processes are in place.
- Will work with relevant staff to address any online safety incidents.
- Will ensure that any online safety incidents are logged and dealt with appropriately in line with the school's Behaviour Policy, Child Protection Policy and / or any other relevant policy.

This list is not intended to be exhaustive.

5.4 Online Safety Lead responsibilities

The Deputy Head Teacher will fulfil this role. The Online Safety Lead will:

- Work closely on a day-to-day basis with the DSL.
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.
- Have a leading role in establishing and reviewing the school's Online Safety Policy and any other additional documentation.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- 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.
- Ensure that there is a system in place for monitoring.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- Liaise with technical staff, pastoral staff and support staff (as relevant).
- Provide (or identify sources of) training and advice for staff / governors / parents / carers / guardians / learners.
- Meet regularly with Governors to review (anonymized) incidents and filtering and monitoring logs and discuss current issues.
- Attend relevant Governor meetings / groups.
- Report regularly to the Head Teacher.

This list is not intended to be exhaustive.

The Designated Safeguarding Lead, Online Safety Lead and other Senior Leaders should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Sexting (see appendix Advice for Schools: Responding to and Managing Sexting Incidents and appendix Gov.uk guidance: Sharing Nudes and Semi-Nudes).
- Inappropriate online contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

This list is not intended to be exhaustive.

5.5 Network Manager responsibilities

The school has a technology service provided by an outside contractor. The school is responsible for ensuring 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 the school's Online Safety Policy and procedures.

Network Managers are responsible for ensuring that:

- They are aware of and follow the school's Online Safety Policy when carrying out their work.
- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the local authority.
- 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 so that any misuse / attempted misuse is reported to the DSL and Online Safety Lead for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring software / systems are implemented and regularly updated as agreed in school policies.
- All software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.

This list is not intended to be exhaustive.

5.6 All staff and volunteers' responsibilities

All staff, including contractors, agency staff and volunteers are responsible for ensuring that:

- They have an awareness of current online safety matters / trends and of the current Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They have read, understood and signed the staff AUA / community user AUA on the school sign in system, before they are provided with access to school systems.
- They immediately report, in person, any urgent suspected misuse or problem to the DSL and Online Safety Lead.
- They immediately report all suspected misuse or problems to the DSL Lead and Online Safety Lead, using CPOMS for investigation / action, in line with the school safeguarding procedures.
- They identify sexting incidents, manage them and escalate appropriately (see appendix Advice for Schools: Responding to And Managing Sexting Incidents).
- They respond appropriately to all reports and concerns about sexual violence and / or harassment, both online and offline, and maintain an attitude of 'it could happen here'.
- All digital communications with pupils and parents, guardians and / or carers are on a professional level and only carried out using official school systems.
- They ensure learners understand and follow the Online Safety Policy and learner AUA, 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 should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safer Remote Learning Resource.
- They have a zero-tolerance approach to incidents of cyber-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.
- Online safety issues are embedded in all aspects of the curriculum and other activities.

This list is not intended to be exhaustive.

5.7 Parents, guardians and / or carers' responsibilities

Parents, guardians 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 takes every opportunity to help parents, guardians and carers understand these issues by:

- Publishing the school's Online Safety Policy on the school website
- Providing them with a copy of our Learners AUA.
- Publishing information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images etc.
- Meetings, newsletters, the school website, social media, literature and any other relevant information about national / local online safety campaigns.

Parents and carers are encouraged to support the school in reinforcing the online safety messages provided to learners in school. This list is not intended to be exhaustive.

6. Educating pupils about online safety

Teachers will work with the Online Safety Lead and the Computing Curriculum Lead to develop a planned and coordinated online safety education programme using the Project EVOLVE programme and resources. This will be provided through:

- A programme of discrete weekly online safety lessons in all Key Stage 1 (KS 1) and Key Stage (KS 2) classes. The school use a bespoke tracker to record when lessons have been completed.
- Personal, Health, Social Education (PSHE) and Relationships and Sex Education (RSE) programmes.
- Assemblies.
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

All schools have to teach:

- Relationships, Health Education (RHE) in primary schools.

In KS 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In KS 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.
- Be discerning in evaluating digital content.

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.

- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.
- What sorts of boundaries are appropriate in friendships with peers and others (including online). This can include learning about boundaries in play and in negotiations about space, toys, books, resources etc.
- The concept of privacy and its implications for both children and adults; including that it is not always right to keep secrets if they relate to being safe.
- That each person's body belongs to them, and the differences between appropriate and inappropriate or unsafe contact, including physical contact.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online), including those they do and do not know.
- How to recognise when a relationship is harmful or dangerous, including skills for recognizing who to trust and who not to trust.
- How to report abuse, concerns about something seen online or experienced in real life, or feelings of being unsafe or feeling bad about any adult and the vocabulary and confidence needed to do so.
- How to ask for advice or help for themselves or others, and to keep trying until they are heard. Where to get advice e.g. family, school and/or other sources.
- That for almost everyone the internet is an integral part of life. Pupils should be supported to think about positive and negative aspects of the internet.
- Pupils should be supported to discuss how online relationships can complement and support meaningful in-person relationships, but also how they might be in tension, and the reasons why online relationships are unlikely to be a good substitute for high quality in-person relationships, looking at the pros and cons of different ways of using online connection.
- The benefits of limiting time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- How to consider the impact of their online behaviour on others, and how to recognise and display respectful behaviour online.
- Why social media, some apps, computer games and online gaming, including gambling sites, are age restricted.
- The risks relating to online gaming, video game monetization, scams, fraud and other financial harms, and that gaming can become addictive.
- How to take a critical approach to what they see and read online and make responsible decisions about which content, including content on social media and apps, is appropriate for them.
- That abuse, bullying and harassment can take place online and that this can impact

wellbeing. How to seek support from trusted adults.
- How to understand the information they find online, including from search engines, and know how information is selected and targeted.
- That they have rights in relation to sharing personal data, privacy and consent.
- Where and how to report concerns and get support with issues online.

At Wellington Primary School we:

- Use Project EVOLVE, a planned online safety curriculum, for all year groups matched against the nationally agreed framework – Education for a Connected World Framework – developed by UKCIS/DCMS, taught in weekly lessons.
- Ensure lessons are matched to need; are age-related and build on prior learning.
- Ensure lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Ensure learner need and progress are addressed through effective planning and assessment.
- Ensure digital competency is planned and effectively threaded through other curriculum areas e.g. PHSE, RSE etc.
- Incorporate / make use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- Ensure 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 (EAL).
- Ensure learners should be helped to understand the need for the learner AUA and encouraged to adopt safe and responsible use online, both within and outside school.
- Ensure staff act as good role models in their use of digital technologies, the internet and mobile devices.
- Ensure 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.
- Ensure where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.
- Accept 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).
- Ensure the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

7. Training

At Wellington Primary School, training is a fundamental part of the school's approach to online safety.

7.1 Staff / volunteers training

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

- A programme of annual online safety and data protection training (E Safety and General Data Protection) will be completed by all staff.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff training time.
- All new staff will receive online safety and data protection training as part of their

induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements, including references to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The DSL and Online Safety Lead will receive regular updates by reviewing guidance documents released by relevant organizations.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

7.2 Governor training

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 or other relevant organization.
- Participation in school training / information sessions for staff or parents.

7.3 Parents, guardians and / or carers training

The school will seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising and engagement on online safety issues.
- Opportunities for engagement with parents, guardians, carers on online safety issues through parent awareness workshops.
- Learners who are encouraged to pass on to parents the online safety messages they have learned in lessons.
- Letters, newsletters and the school website.
- High profile events / campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites / publications, e.g. SWGfL, www.saferinternet.org.uk/ and www.childnet.com/parents-and-carers.

7.4 Visitors and members of the community training

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.
- The school will provide online safety information via their website and social media for the wider community.

8. Acceptable Use

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

8.1 Acceptable Use Agreement (AUA)

The Online Safety Policy and AUA define acceptable use at the school. The AUA are communicated / re-enforced through:

- Staff induction and handbook.
- Posters / notices around where technology is used.
- Communication with parents, guardians and carers.
- Education sessions.

- The school website.
- Peer support.

8.2 Guidance for Members of the School Community

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 but not limited to:

- 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 including harassment and stalking.
- Drug-related offences.
- Weapons / firearms offences.
- fraud and financial crime including money laundering.

Users shall not undertake activities that might be classed as **cyber-crime** under the Computer Misuse Act (1990) for example:

- 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.
- Gaining unauthorised access to school networks, data and files, through the use of computers/ devices.
- Creating or propagating computer viruses or other harmful files.
- Revealing or publicizing 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).

The DSL, Online Safety Lead and Senior Leaders will decide whether **infringements** will be dealt with internally or by the police. Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda, the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways.

Users shall not undertake activities that are **not illegal but are classed as unacceptable** in school policies for example:

- Accessing inappropriate material / activities online in a school setting including pornography, gambling, drugs (informed by the school's filtering practices and / or AUA).
- Promotion of any kind of discrimination.
- Using school systems to run a private business.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Infringing copyright.
- Unfair usage (downloading / uploading large files that hinder others in their use of the internet).
- Any other activity which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute.

Work devices must be solely used for work activities.

When using **personal devices**, the school considers the following as good practice:

Pupils:

- learners should switch of their mobile phones off when they get to the school gate and they should not turn them on again until they get to the school gate to leave at home time.
- learners should hand their mobile phones in, for safe keeping, when they arrive at school, and collect them at the end of the school day.
- learners should not use their own personal devices (mobile phones / smart watches / USB devices etc.) in school.

Staff, governors and volunteers:

- Users may bring mobile phones to school.
- Users shall not bring other personal devices to school e.g. cameras / tablets / gaming devices.
- In areas / rooms where learners are present (including during break times, off site and residential visits) users shall keep their mobile phones out of sight and set to "silent". Users shall not use their mobile phones for any purpose, including telling the time.
- Users shall not take photos or video footage on any mobile phone / personal device (even when the photos or videos are intended for publication beyond the school or online).
- The school acknowledges that there may be exceptional circumstances when a user may need to be contactable during the school day e.g. when a close family member is ill; at such times the user should keep their mobile phone out of sight but set to "ring" and they should step out of class into an area where learners are not present, to take any emergency calls. The school also recognizes that mobile devices may be used for multi-factor authentication when logging into Outlook and CPOMS.

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 users and learners or parents, guardians and / or carers (via e-mail / 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.
- School e-mail should not be used for personal e-mails.
- Users are expected to follow good practice when using personal social media to protect their own professional reputation and that of the school and its community.
- Users will follow all guidance issued, when contributing to the school's use of social media, as an official communication channel.
- Users should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, to the DSL and Online Safety Lead, and they must not respond to any such communication.
- Relevant policies and permissions are followed when posting information online e.g. on the school website and school social media accounts.

9. Reporting and responding

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

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. All members of the school community are made aware of the need to report online safety issues / incidents.
- Reports are dealt with as soon as is practically possible once they are received.
- 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 to relevant agencies.
- Any concern about staff misuse will be reported to the DSL and Online Safety Lead, unless the concern involves the DSL and / or Online Safety Lead, in which case the complaint will be referred to the Chair of Governors and the Local Authority Designated Officer (LADO).
- Devices may be searched and confiscated where there are reasonable grounds for suspecting: content poses a risk to staff and / or pupils; is identified in the school rules as a banned item for which a search can be carried out; and / or is evidence in relation to an offence.
- Before a search is authorised, at least two senior members of staff should be involved in this process (this is vital to protect individuals if accusations are subsequently reported). In addition, staff should explain why the person is being searched, how the search will happen, and allow them an opportunity to ask questions about it.
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image) they will not view the image. They will confiscate the device and report the incident to the DSL and Online Safety Lead immediately.
- **Any urgent suspected misuse or problem** should be reported immediately, in person, to the DSL and Online Safety Lead.
- **All suspected misuse or problems** should be reported immediately to the DSL and Online Safety Lead, using CPOMS for investigation / action, in line with the school's safeguarding procedures.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. the Local Authority Designated Officer, the police; the Professionals Online Safety Helpline, the Report Harmful Content website and the Child Exploitation and Online Protection (CEOP) website.
- Those involved in an incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Follow up from an incident (or pattern of incidents) will take place (as relevant) to:
    - Staff, through regular communications.
    - Learners, through assemblies / lessons.
    - Parents, guardians and carers, through newsletters, school social media, the school website.
    - Governors, through regular safeguarding updates.
    - Local authority / external agencies, as relevant.
- For further information, please see DfE guidance Searching, Screening and Confiscation.

9.1 Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (Please also refer to the school's Anti-Bullying Policy and Behaviour Policy).

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather

than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's Anti-Bullying Policy and Behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.

9.2 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents, guardians and carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

As a school, we recognise that AI has many uses to help pupils learn, but may also have the potential to be used to negatively and to cause harm or distress to others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. As a school, we will treat any use of AI to bully pupils very seriously, in line with our Anti-Bullying Policy and Behaviour Policy. The rise of AI and how to use it appropriately, is also built into the school's online safety education work.

Staff should be aware of the risks of using AI tools whilst they are still being developed, including data protection compliance.

9.3 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, possible incidents:

- Deliberately accessing or trying to access material that could be considered illegal (see list above).
- Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access the school network by sharing username and passwords.
- Corrupting or destroying the data of other users.
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.
- Unauthorised downloading or uploading of files or use of file sharing.
- Using proxy sites or other means to subvert the school's filtering system.
- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Deliberately accessing or trying to access offensive or pornographic material.
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.
- Unauthorised use of digital devices (including taking images).

- Unauthorised use of online services.
- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.
- Continued infringements of the above, following previous warnings or sanctions.

Possible sanctions:

- Refer to class teacher.
- Refer to DSL and Online Safety Lead.
- Inform parents / carers.
- Remove device / network / internet access rights.
- Issue a warning.
- Further sanction, in line with Behaviour Policy.
- Refer to Local Authority / Technical Support Staff for action re filtering, etc.
- Refer to Local Authority.
- Refer to police / social services.

Responding to staff, volunteer, visitor actions, possible incidents:

- Deliberately accessing or trying to access material that could be considered illegal (see list above).
- Deliberate actions to breach data protection or network security rules.
- Deliberately accessing or trying to access offensive or pornographic material.
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.
- Using proxy sites or other means to subvert the school's filtering system.
- Unauthorised downloading or uploading of files or file sharing.
- Breaching copyright or licensing regulations.
- Allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.
- sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.
- Using personal e-mail / social networking / messaging to carry out digital communications with learners or parents / carers.
- Inappropriate personal use of the digital technologies e.g. social media / personal e-mail.
- Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner.
- Actions which could compromise the staff member's professional standing.
- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.
- Failing to report incidents whether caused by deliberate or accidental actions.
- Continued infringements of the above, following previous warnings or sanctions.

Posisble sanctions:

- Refer to DSL and Online Safety Lead.
- Issue a warning.
- Disciplinary action.
- Suspension.
- Refer to Local Authority / Technical Support Staff for action re filtering, etc.
- Refer to Local Authority.
- Refer to Police.

10. Technology

It is the responsibility of the school to ensure that the technology provider / network manager carries out all the online safety and security measures that would otherwise be the responsibility of the school. 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.

The school ensures that the technology provider / network manager is fully aware of the school Online Safety Policy and acceptable use agreements. The school has a Data Processing Agreement in place with them.

10.1 Filtering

- The school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents / behaviours and are based on the DfE's Meeting Digital and Technology Standards in Schools and Colleges (2023) guidance.
- The school manages access to content across its systems for all users.
- The filtering provided meets the standards defined in the UK Safer Internet Centre - Guide for Education Settings and Filtering Providers.
- Access to online content and services is managed for all users.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband and filtering provider.
- There are established and effective routes for users to report inappropriate content.
- There is a clear process in place to deal with requests for filtering changes.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users: staff / learners).
- Younger learners will use child friendly / age-appropriate search engines.
- Filtering logs are regularly reviewed and the school provider alerts the school to breaches of the filtering policy, which are then acted upon.
- 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 SWGfL Report Harmful Content site.

10.2 Monitoring

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

- The school monitors all internet use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored.
- The DSL and Online Safety Lead are responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse / misuse.
- There is a clear process for prioritizing response to alerts that require rapid safeguarding intervention; management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Technical monitoring systems are up to date and managed and logs / alerts are regularly

reviewed and acted upon.

The school follows the DfE's Meeting Digital and Technology Standards in Schools and Colleges (2023) guidance, as well as the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies:

- physical monitoring (adult supervision in the classroom).
- internet use is logged, regularly monitored and reviewed.
- filtering logs are regularly analyzed and breaches are reported to the DSL and Online Safety Lead.

10.3 Technical Security

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

- 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.
- There are rigorous and verified back-up routines, including the keeping of network-separated copies off-site.
- All users have clearly defined access rights to school technical systems and devices; details of the access rights available to groups of users are recorded by the Network Manager and are reviewed, at least annually, by the Online Safety Lead.
- All users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details; users must immediately report any suspicion or evidence that there has been a breach of security.
- All school networks and systems are protected by secure passwords; the passwords must not be shared with anyone.
- The master account passwords for the school systems are kept in a secure place.
- The Network Manager is responsible for ensuring that all software purchased by and used by the school is adequately licensed 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.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data; these are tested regularly.
- The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- An agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / learners / community users) are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media on school devices. systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

10.4 Digital Media, the School Website and Social Media

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

- Ensuring that personal information is not published.
- Providing education / training including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Having clear reporting guidance, including responsibilities, procedures and sanctions.
- Assessment of risk, including legal risk.
- Guidance for learners, parents / carers.

School staff should ensure that:

- No reference should be made in social media to learners, parents, guardians and 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 minimize 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 is:

- 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.
- An understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use:

- Personal communications are those made, for example, via personal social media accounts.
- Personal accounts must not be used to associate users with / impact on the school.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- The school permits staff reasonable and appropriate access to personal social media sites during school hours i.e. during break and lunch times.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media:

- As part of active social media engagement, the school pro-actively monitors the internet for public postings about the school.
- The school effectively responds to social media comments made by others.
- When parents, guardians and / or 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.

10.5 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, guardians, carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place, amongst other things. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff 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.
- Images should only be taken on school devices; the personal devices of staff should not be used for such purposes.
- In accordance with Taking Photographs: Data Protection Advice For Schools (guidance from the Information Commissioner's Office website) parents, guardians and / or 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 the Online Safety Policy.
- Learners' full names will not be used anywhere on the school website or social media, particularly in association with photographs.
- Written permission from parents, guardians and / or carers will be obtained before photographs of learners are taken for use in school or published on the school website / social media.
- Parents, guardians and / or 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, guardians and / or carers.

10.6 Online Publishing

The school communicates with parents, guardians and / or carers and the wider community and promotes the school through:

- Our school website, including newsletters.
- Social media.

The school website is managed by the Deputy Head Teacher. The school ensures that the Online Safety Policy has been followed in the use of online publishing e.g. in the 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 images or videos are published, their identities are protected; their names are not published. Where learner work is published, their identities are protected, only first names are published.

10.7 Data Protection

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

The school:

- 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.
- The 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, guardians, carers, volunteers and children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix).
- Has procedures in place to deal with the individual rights of the data subject.
- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data.
- Reports any relevant breaches to the Information Commissioner within 72 hours 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 (FOI) Policy which sets out how it will deal with FOI requests.
- Provides data protection training for all staff at induction and appropriate refresher training

thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data will be encrypted, and password protected.
- Device will be password protected.
- Device will be protected by up-to-date endpoint (anti-virus) software.
- Data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.
- Can recognize 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.

11. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated:

- There is balanced professional debate about the evidence taken from 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, guardians and / or 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 relevant agencies to help ensure the development of a consistent and effective local online safety strategy.

APPENDICES

The appendices are as follows:

- Acceptable Use and Cloud Agreement EYFS, KS1 pupil
- Acceptable Use and Cloud Agreement KS2 pupil
- Acceptable Use Agreement Staff and Volunteers
- DPO Impero DPO Service by SAMPeople
- GDPR Pact HR policy
- Online safety in schools and colleges (governing body questions)
- Photos, video and work permissions for pupils who have left school (pages 1 and 2)
- Sexting (managing incidents)
- Sharing nudes and semi-nudes (advice for Education settings)
- Sharing nudes and semi-nudes (how to respond to an incident)
- Use of social media (concern outside school letter home)
- Social media advice for staff