On-Line Safety and Acceptable Use Policy

This policy applies to all members of the Steephill School community, including the EYFS setting.

Policy Author: Helen Millward, Headteacher: September 2025

Next Review: September 2026

Related documents:

Meeting digital and technology standards in schools and colleges - Guidance

Policy statement

Steephill School recognises that digital and online technologies play an important role in education and in the lives of pupils, staff and parents. Used correctly, they enhance learning, communication, and collaboration. However, misuse can pose risks to safeguarding, wellbeing, reputation, and compliance with the law.

This policy ensures that pupils, staff, governors, parents and visitors understand their responsibilities in using technology safely and respectfully. It sets out how the school teaches online safety, manages digital systems, and responds to concerns.

The policy aligns with:

1. Keeping Children Safe in Education (KCSIE) 2025,
2. Working Together to Safeguard Children (2023)
3. UK GDPR and Data Protection Act 2018
4. Prevent Duty 2015
5. Independent School Standards (ISSR)
6. National Guidance for Independent Schools

This policy applies to all digital technologies, including school networks, devices, email, messaging, internet, intranet, cloud services, and personal devices used for school purposes.

Aims

- To ensure that pupils and staff use technology safely and responsibly and that online safety is embedded across the curriculum.
- To protect and safeguard pupils from online risks and harm including bullying, exploitation, and exposure to inappropriate content.
- To promote responsible, respectful and safe use of digital technology.
- To provide guidance and establish clear acceptable use expectations for pupils, staff, parents and visitors.
- To ensure appropriate and robust filtering and monitoring systems are in place.
- To provide a framework for education, reporting, and responding to online safety incidents.
- To support the teaching of digital literacy and online safety across the curriculum
- To fulfil all statutory duties in relation to safeguarding and data protection.
- To ensure all incidents are recorded, reviewed, and responded to appropriately.

This policy applies to:

- Pupils (EYFS–KS2)
- Staff and volunteers
- Governors
- Parents and carers
- Visitors using school systems or devices

It applies to:

- Use of school devices and networks (on or off-site)
- Use of personal devices where they access school data, communication, or platforms
- Behaviour online that may impact pupils, staff, or the school's reputation

Roles and Responsibilities

Governors

- Ensure an effective online safety policy is in place.
- Ensure effective filtering and monitoring systems are in place.
- Appoint a governor with oversight of online safety.
- Ensure online safety is integrated into safeguarding and curriculum monitoring.
- Review termly reports on incidents, trends, and actions taken.

Headteacher (also acting as Online Safety Lead)

- Overall responsibility for online safety and acceptable use.
- Ensure policy implementation and annual review.
- Oversee filtering and monitoring effectiveness and response to incidents.
- Ensure staff receive regular training.
- Ensure pupils receive education in online safety.
- Oversees SENSO alerts and reporting procedures.
- Update staff, governors, and pupils on emerging risks.
- Liaise with external agencies (LA, ISI, Ofsted, police) where required.

Designated Safeguarding Lead (DSL)

- Monitors, investigates, and responds to online safety incidents.
- Maintains records of all concerns and actions taken.
- Liaises with external agencies when required.

Staff and Volunteers

- Model safe and responsible behaviour.
- Follow the Acceptable Use Agreement.
- Report online concerns to the DSL immediately and record on CPOMS.
- Use school devices and platforms for professional communication only.

Pupils

- Follow the Pupil Acceptable Use Agreement.
- Report anything that makes them feel worried or unsafe.
- Use technology responsibly and respectfully.

Parents and Carers

- Support safe use of technology at home.
- Follow the Parent Acceptable Use Agreement.
- Respect school guidance on sharing photos, videos or comments on social media.

Education and Training

Pupils: Online safety is embedded in the curriculum across all Key Stages predominantly Computing, PSHE, assemblies and cross-curricular lessons. Focus areas include cyberbullying, managing online relationships, social media, digital resilience, privacy, gaming, screen time, and recognising risk.

Staff: All staff receive annual online safety training linked to safeguarding. Updates are provided on new risks, safeguarding procedures or following national/local incidents.

Parents: The school provides guidance on home filtering, gaming, social media, and parental controls through workshops, newsletters, and the school website.

Acceptable use

Pupils

- Use school devices, accounts and internet for learning only.
- Keep personal login details private.

- Never share personal information online.
- Tell a trusted adult if they see something worrying.
- Be kind and respectful online (no cyberbullying, trolling, or harmful content).
- Mobile phones are not permitted on school site at anytime.

Staff

- Use school email, devices, and platforms for all professional communication only.
- No use of personal phones for photographing/videoing pupils.
- Store and share pupil data securely in line with GDPR.
- Ensure personal devices used for school purposes are secure. All devices must be locked when unattended.
- Report data breaches or safeguarding concerns immediately.
- Maintain professional boundaries on social media. Personal social media profiles must be private and use must not bring the school into disrepute.

Parents

- Support school guidance on online safety at home.
- Not share school-related images, videos, or comments on social media.
- Communicate with staff via school-approved channels only.
- Respect staff boundaries (no direct social media messaging).

Visitors

- Follow guidance for safe online communication with school.
- Report concerns to staff promptly.

Filtering and monitoring

The school uses SENSO, an online monitoring and safeguarding solution, to provide real-time oversight of pupil activity on school devices.

SENSO automatically alerts designated safeguarding staff with real-time monitoring with automatic alerts for risks concerning online behaviour, safeguarding risks, or attempts to access inappropriate content.

Age-appropriate web filtering is applied to all school devices and internet access to block harmful or unsuitable content, in line with DfE and KCSIE requirements.

Monitoring reports and alerts are reviewed by the DSL (and Online Safety Lead) to ensure timely action is taken when concerns are raised.

The Headteacher and Governors review annually of the effectiveness of SENSO monitoring and filtering systems.

Filtering and monitoring arrangements are reviewed termly to ensure they remain appropriate and effective.

This monitoring applies to all school devices and accounts, on or off-site.

Staff and pupils are aware that usage is monitored.

Personal devices are guided for safe use but not directly monitored.

Responding to concerns and incidents

The DSL will investigate and act on all online safety concerns. All incidents must be reported immediately to the DSL. All concerns must be logged on CPOMS. The school will escalate concerns to external agencies where required (e.g., police, CEOP). Pupils involved in online safety incidents will receive support through pastoral care and, where appropriate, sanctions.

Escalation Flowchart:

1. Incident identified → staff member informs DSL
2. DSL assesses risk → record in CPOMS
3. Action taken → pastoral support, sanctions, parental involvement
4. External escalation → police, CEOP, or other agency if required
5. Review & follow-up → Online Safety Lead reports termly to governors

- Cyberbullying – will be dealt with using the Positive Behaviour Policy and Anti Bullying Strategy.
- Sexting / sharing inappropriate images - referred to safeguarding and external agencies.
- Online radicalisation / Prevent concerns - referred to the DSL and, if required, the Channel programme.
- Inappropriate contact or grooming - referred to the DSL and police if necessary.
- Data breaches - referred to the Head and Data Protection Officer, with ICO notification if required.

Breaches of Policy

Pupils: sanctions in line with the Positive Behaviour Policy (e.g. loss of device use, parental meeting, suspension for serious breaches).

Staff: disciplinary action in line with the Staff Code of Conduct.

Parents/Visitors: breach of expectations may result in restricted access to school communication or site.

Record keeping & confidentiality

- All online safety incidents are logged by the DSL and stored securely.
- Annual audit of SENSO and filtering systems.
- Records are kept for at least 7 years in line with data retention.
- Confidentiality is maintained except where information must be shared for safeguarding or legal reasons.

Data Protection

Staff and pupils must follow GDPR and data protection laws which comply with the Data Protection Act 2018 / GDPR.

Personal data is stored securely and only accessed by authorised personnel.

Any breaches are reported in line with the Data Protection Policy.

Personal data will be recorded, processed, transferred and made available according to the GDPR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the GDPR.
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.
- 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 and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete.

Remote learning and off-site use

Online safety standards apply to remote learning and online collaboration.

Staff ensure live lessons and video calls are secure.

Pupils and parents are provided guidance on responsible use of digital platforms at home.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- 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 General Data Protection Regulations - GDPR). 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 pupils 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, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or social media pages that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Photographs published on the website, or social media pages must be checked prior to posting.

- Pupils' names will not be used anywhere on a website, social media page or blog, particularly in association with photographs.

- Written consent from parents or carers will be obtained before photographs of pupils are published on the school website, social media pages or weekly newsletters.

- Pupils' work can only be published with the permission of the pupil and parents or carers.

Communication with pupils

Within computing lessons at school, there may be some appropriate communication between staff and pupils electronically, for example receiving homework, photos or emails. This should not be used with EYFS.

Staff must ensure that communication with pupils is within clear and explicit professional boundaries. Inappropriate communication via telephone, email, text or social networking sites between an adult and a child under the age of 18 outside of professional protocol may lead to disciplinary action. Misuse or abuse of these guidelines would also be construed as gross misconduct; this could lead to dismissal and be reported to the appropriate Safeguarding Body including OFSTED and the Disclosure and Barring Service (DBS).

If any pupil should communicate with a member of staff via a personal email account or social media, the member of staff should not reply and report this to the Head immediately.

Child on Child abuse – including online

This is highlighted in KCSIE 2024 and it is important to have a culture of understanding that there is never 'just banter' but that any hurtful or sexual remarks can have serious consequences and should be taken seriously. Child on child abuse is dealt with in more detail in the Safeguarding Policy.

Social Media

Steephill School has a duty of care to provide a safe learning environment for pupils and staff. The school could be held indirectly responsible for acts of its employees in the course of their employment. Staff members who harass, cyberbully, 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.

Social networks are web-based communication structures that enable easy communication and relationship building between individuals via the Internet, many of which include additional access to further methods of interaction, such as e-mail and instant messaging. While we at the School consider the widespread use of social networking applications an effective and useful method for communication in the appropriate context, the potential for misuse by workers, during and out of work hours, is such that the following guidelines are in place.

Social networks include, but are not limited to WhatsApp, Facebook, Tik Tok, Instagram, Twitter, Snapchat, LinkedIn, and personal blogs.

This social networking policy has the following purpose:

- to help protect the School against potential liability;
- to give employees clear guidance on what can and cannot be said about the School or other workers;
- to help line managers effectively manage employee performance, time management and use of the School's resources;
- to help workers separate their professional and personal communication;

- to comply with the law on discrimination, data protection and protecting the health of employees; and
- to be clear about the use of monitoring within the School.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

School staff must ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community;
- They do not comment or express opinions on other employees of the school, the leadership of the school, governors of the school, or school policy;
- They do not join social media groups with parents of the school, including Facebook and WhatsApp groups;
- 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.

The school's use of social media for professional purposes will be checked regularly by the Head to ensure compliance with school policies.

Breaches to this policy may mean that the disciplinary procedure will take effect.

Online Sexual Violence and Sexual Harassment

Our Safeguarding policy explains our response to incidents of sexual violence and sexual harassment.

Support is available to schools (taken from Sexual Violence and Sexual Harassment between Children in Schools and Colleges):

Steephill School recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services, and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than our school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator(s)) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

- The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues and will be especially useful for the designated safeguarding lead (and their deputies) when a report of sexual violence or sexual harassment includes an online element.
- Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.
- Childline/IWF Remove a nude image shared online Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online, to see if they can be removed from the internet.
- UKCIS Sharing nudes and semi-nudes advice: Sharing indecent images of a child (including by children) is a crime. UKCIS Sharing nudes and seminudes: advice for education settings working with children and young people provides support in responding to reports of children sharing nonconsensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery). Please see footnote 17 for further information.
- Thinkuknow from NCA-CEOP provides support for the children's workforce, parents and carers on staying safe online.

Expanded Online Safety Risks

In line with current statutory guidance, including *Keeping Children Safe in Education (KCSIE)*, the school recognises that online safety risks continue to evolve. In addition to the established categories of risk (content, contact, and conduct), we now explicitly include **content risks** linked to disinformation, misinformation, and conspiracy theories.

These risks can:

- Expose children to inaccurate, harmful, or misleading information.
- Undermine trust in reliable sources and authorities.
- Influence children's understanding of world events, relationships, or health and wellbeing.
- Lead to increased vulnerability to exploitation, radicalisation, or harmful decision-making.

School Approach

- **Curriculum:** Online safety education, delivered through Computing, PSHE, and across the wider curriculum, will include age-appropriate teaching on identifying reliable sources, fact-checking, critical thinking, and digital resilience.
- **Staff Training:** All staff will be trained to recognise the signs that a pupil may have been exposed to harmful misinformation, disinformation, or conspiracy theories and will know how to respond in line with safeguarding procedures.
- **Parental Engagement:** Parents/carers will be provided with guidance and resources to help them support their child's safe and critical use of online content at home.
- **Pupil Voice:** Children will be encouraged to speak openly about what they see or hear online, including content they find confusing, upsetting, or contradictory.

- **Safeguarding Response:** Any concerns that a pupil has been adversely affected by harmful or misleading online content will be treated as a safeguarding matter and managed in accordance with the school's safeguarding procedures.

Planning Technology to Support Safeguarding and Online Safety

We recognise that technology planning is an essential part of safeguarding, online safety, and the prevention of cyber incidents. All digital systems, devices, and platforms will be assessed and implemented with the welfare of pupils in mind.

Planning and Assessment

- We will use the **"Plan technology for your school" self-assessment tool** (as referenced in paragraph 142 of national guidance) to:
    - Review existing IT systems and digital infrastructure.
    - Identify potential risks to pupils and staff, including cybersecurity threats and online safety vulnerabilities.
    - Ensure technology aligns with safeguarding policies, procedures, and legal obligations.
- The assessment will cover areas such as network security, device management, access controls, monitoring tools, and online safety features.

Roles and Responsibilities

- Leadership Team: The senior leadership team will oversee the strategic use of technology and ensure that safeguarding is embedded in all digital planning decisions.
- IT/Technical Staff: Responsible for implementing recommendations from the self-assessment tool, maintaining secure systems, and monitoring digital safety measures.
- Designated Safeguarding Lead (DSL): Will work closely with IT and leadership teams to ensure that technology planning supports safeguarding and online safety goals.

Review and Improvement

- Technology planning and assessments will be conducted regularly (at least annually) or whenever significant changes to the digital environment occur.
- Outcomes of the self-assessment will inform:
    - Updates to the Online Safety Policy.
    - Staff training and pupil education on safe technology use.
    - Incident response and safeguarding procedures relating to digital systems.

By embedding technology planning into safeguarding procedures, the school ensures a proactive approach to online safety, cyber incident prevention, and the responsible use of digital tools.

Resources:

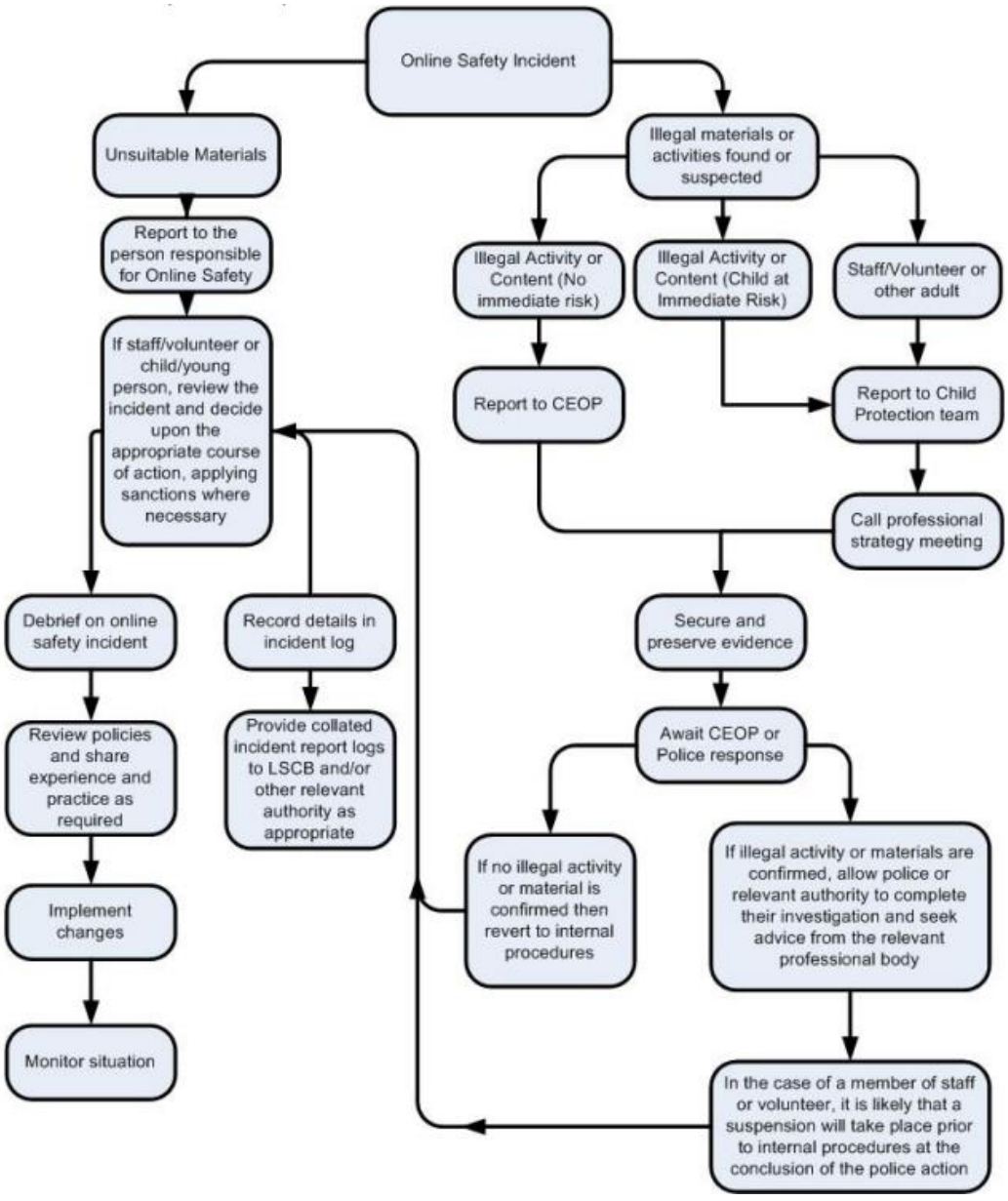
- “Plan technology for your school” self-assessment tool – GOV.UK / Safeguarding Network.

Responsibility

The Designated Safeguarding Lead (DSL) will ensure that the school’s online safety provision remains up to date and reflects emerging risks and national guidance. The DSL will also coordinate with curriculum leads and the school’s online safety coordinator to ensure staff, pupils, and parents are informed and supported.

Responding to illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Responding to other incidents of misuse

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below).
- 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 or national / local organisation (as relevant).
- Police involvement and/or action.
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Acceptable use of technology

Access to email and the Internet is provided during working hours for the purpose of effectively completing work and use must comply with all School policies and procedures.

The School will not tolerate employees using social networking sites for unofficial or inappropriate uses. Specifically:

- you should not use such sites during contracted working hours for personal interest/benefit, without the authority of an appropriate manager. Usage during your agreed breaks is permitted, subject to the rules contained in this policy;
- you should not at any time upload photographs to your social networking sites of yourself any pupil or any other employee taken in a work situation or in a work uniform;
- no defamatory comments about the School should be made on such sites at any time;
- you should not at any time include information that identifies any other employee/contractor/supplier/client/customer or any other individual working in connection with us;
- you should not at any time express opinions on such sites which purport to be the opinion of the School, nor comments representing your own views on our School;
- any personal blogs should contain a disclaimer that the views expressed on it are personal views of the author only;
- you should not at any time make comments on such sites which bring the School into disrepute;
- you should not at any time make comments on such sites which amount to bullying, harassment or any other detriment towards other employees/ contractors/suppliers/clients/customers or any other individual working in connection with us;
- you should not be 'friends' or join social networking groups with any parent or pupil of the School, or with any ex-pupil under 18 years old; this includes Facebook and WhatsApp groups;
- you should not use instant messaging whether on a PC or by any other means for personal interest during working hours;
- you should not be in contact with any pupil or ex-pupil under 18 years of age.

Acceptable use of the internet

- personal use in working hours or inappropriate use of the internet system may result in disciplinary action which could result in summary dismissal.
- the internet system is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:
  - comply with all of our internet standards;
  - access during working hours should be for business use only;
  - private use of the internet should be used outside of your normal working hours but may be used during breaks subject to this policy.

- the School will not tolerate the use of the Internet system for unofficial or inappropriate purposes, including:
  - accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;
  - non-compliance of our social networking policy;
  - connecting, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material;
  - engaging in computer hacking and other related activities, or attempting to disable or compromise security of information contained on the School's computers.

  You are reminded that such activities may constitute a criminal offence.

Acceptable use of Generative Artificial Intelligence (AI)

We recognise the growing use of generative AI tools (e.g. chatbots, image generators, and automated content creation tools) in education and beyond. While these technologies can provide opportunities for learning, creativity, and efficiency, they also present safeguarding, ethical, and data-protection risks that must be carefully managed.

Risks of Generative AI

Generative AI tools may:

- Produce inaccurate, biased, or misleading information that appears credible.
- Generate harmful or inappropriate content if prompts are misused.
- Involve the sharing of personal or sensitive data, raising privacy concerns.
- Contribute to issues of plagiarism, academic dishonesty, or lack of digital integrity.
- Amplify risks linked to misinformation, disinformation, and online manipulation.

School Approach

- Curriculum: Pupils will be taught, at an age-appropriate level, about how generative AI works, its benefits, and its risks. This includes the importance of critical thinking, verifying AI outputs, and recognising that not all generated content is reliable or appropriate.
- Staff Training: Staff will receive guidance and training on the safe, ethical, and educational use of generative AI. This includes clear protocols on when and how these tools may be used with pupils.
- Use in School:
  - Generative AI will only be used under staff supervision for specific, curriculum-related purposes.
  - Staff and pupils will not be permitted to enter personal data into generative AI systems.
  - AI-generated content will not replace teacher-led planning, assessment, or decision-making.

- **Safeguarding Response:** Any misuse of generative AI by staff or pupils, including attempts to access harmful content or use tools dishonestly, will be addressed in line with the school's safeguarding and behaviour policies for pupils and the staff handbook.
- **Parental Engagement:** Parents will be provided with information about generative AI, its risks, and how to support children in using such tools responsibly at home.

The Designated Safeguarding Lead (DSL), in partnership with the Computing/Online Safety Lead, will ensure that the school's use of generative AI is in line with current legislation, DfE guidance, NSPCC recommendations, and best practice in safeguarding.

Acceptable use of emails

- Personal use during working hours or inappropriate use of the email system may result in disciplinary action which could include summary dismissal.
- All emails concerning School business must be made using the official email address given to you, ending steephill.co.uk. Personal emails to colleagues or parents on school business are not permitted.
- Emails between any member of staff and a pupil are not permitted unless directly concerning online learning.
- Personal use during breaks is permitted subject to this policy.
- The e-mail system is available for communication and matters directly concerned with the legitimate business of the School. Employees using the e-mail system should give particular attention to the following points:
  - all comply with School communication standards;
  - email messages and copies should only be sent to those for whom they are particularly relevant;
  - email should not be used as a substitute for face-to-face communication or telephone contact. Flame mails (i.e. e-mails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
  - if email is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The School will be liable for infringing copyright or any defamatory information that is circulated either within the School or to external users of the system; and
  - offers or contracts transmitted by email are as legally binding on the School as those sent on paper.
- The School will not tolerate the use of the school email system for unofficial or inappropriate purposes, including:
  - any messages that could constitute bullying, harassment or other detriment;
  - personal use (e.g. social invitations, personal messages, chain letters or other private matters);
  - online gambling;
  - accessing or transmitting pornography;

- transmitting copyright information and/or any software available to the user; or posting confidential information about other employees, the School or its customers or suppliers.

Appendix 1

PUPIL ACCEPTABLE USE AGREEMENT KS1

I will ask an adult if I want to use a computer or iPad.

I will only use websites and apps that my teacher has told me to use.

I will tell an adult if I see something that makes me feel worried or upset.

I will be kind and polite when I use technology.

I know that adults in school will check what I am doing online.

Name:

Date:

Appendix 2

PUPIL ACCEPTABLE USE AGREEMENT KS2
I will use technology responsibly and for learning. I will not share personal information (like my name, address, or password). I will report anything that makes me feel unsafe. I will be respectful when communicating online. I will not use social media or gaming sites in school.
Name:
Date:

Appendix 3

STAFF ACCEPTABLE USE AGREEMENT

I have read and understood Steephill School's full Online Safety policy and agree to uphold the content.

I will immediately report any data breaches or suspicions of safeguarding concerns (by adults or children) in line with the policy without delay.

I understand it is my duty to support a whole-school safeguarding approach and will report and record any behaviour which I believe may be inappropriate or concerning in any way both on CPOMS and to the Designated Safeguarding Lead / Headteacher.

I will only use school devices, accounts, and platforms for professional communication.

I will keep my passwords secure and not share them.

I will ensure data is stored and transferred securely.

I will not use personal devices to photograph pupils.

I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

- not sharing other's images or details without permission
- refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

I understand that in any periods of home learning, school closures or potential lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.

I understand the importance of upholding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either.

I agree to adhere to all provisions of the school Data Protection at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the Headteacher if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

I will not store school-related data on personal devices, storage or cloud platforms. I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.

I understand and support the commitments made by pupils, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Name:
Signed:
Date:

Appendix 4

PARENT ACCEPTABLE USE AGREEMENT

I will support my child in using technology safely at home.

I will not share photos or videos of school events online and ensure that they are for personal use only.

I will use official channels to contact staff.

I will respect staff boundaries and not use social media to raise concerns.

I will immediately report any safeguarding concerns or data breaches.

Name:
Name of child:
Signed:
Date: