



Cheshire Academies Trust

Inspiring hearts and minds

Online Safety Policy

Mill View Primary School

2026-2027

Next update: Autumn 2027

Cheshire Academies Trust. Updated to reflect Keeping Children Safe in Education 2026 (in force 1 September 2026), including revised filtering and monitoring requirements, the four areas of online risk (4Cs), guidance on generative AI, and the DfE's mobile phones in schools statutory guidance.

Contents

1. Scope of this policy	4
2. Policy aims	4
3. Schedule for development, monitoring and review.....	4
4. Roles and responsibilities	5
Local Governing Body	5
Headteacher and senior leaders.....	5
SLT member responsible for filtering and monitoring	5
Online Safety Lead	5
Network manager / technical support	6
Teaching and support staff.....	6
Designated Safeguarding Lead	6
Pupils	6
Parents/carers	7
Community users.....	7
5. Online safety education.....	7
Pupils	7
Parents/carers	8
Staff, governors and volunteers	8
6. The four areas of online risk (the 4Cs).....	9
7. Safer use of technology	9
Generative artificial intelligence (AI)	9
8. Filtering and monitoring.....	10
Devices.....	10
Visitors	10
Images.....	10
9. Mobile phones.....	11
Pupils	11
Staff use of personal devices and mobile phones.....	11
Visitors' use of personal devices	11
10. Data protection and security	11
Access and permissions	11
Passwords and devices	12
Storage of data	12
Secure transfer and remote access	12
11. Social media and communications	12
Communication	12
Staff use of social media.....	13
School use of social media.....	13

12. Reporting and responding to incidents	13
13. Sanctions.....	14
14. Technical infrastructure.....	14
Appendix 1: Staff and Volunteer Acceptable Use Agreement	16
Purpose.....	16
Professional and personal safety.....	16
Professional conduct online	16
Use of devices and data.....	16
Copyright and fair use	16
Responsibilities beyond school.....	17
Declaration	17
Appendix 2: KS1 (Infant) Pupil Acceptable Use Agreement	18
Appendix 3: KS2 Pupil Acceptable Use Agreement	19
Keeping myself safe	19
Respecting others	19
Using technology responsibly.....	19
Research and learning online	19
Taking responsibility.....	19

1. Scope of this policy

This policy applies to all members of the Mill View Primary School community (staff, pupils, volunteers, trainee teachers, parents/carers, visitors, community users) who have access to or use the school's digital technology, systems, networks, internet access or digital communication tools, both on and off site.

It sets out how the school will:

- Protect pupils from online harm in line with the four areas of online risk (the 4Cs: content, contact, conduct, commerce) as outlined in KCSIE 2026
- Embed online safety education within the curriculum
- Ensure that technical systems (filtering and monitoring) are effective and proportionate, and reviewed at least once every academic year
- Manage the safe use of emerging technologies, including generative artificial intelligence (AI)
- Support staff, parents and pupils to build digital resilience

2. Policy aims

- To safeguard pupils from inappropriate online content, harmful contact (including from generative AI applications that simulate harmful interaction), unsafe conduct, and exploitative commerce
- To educate pupils to use technology safely, responsibly and respectfully
- To support staff and parents to understand online risks and their role in promoting safe use
- To ensure robust systems of reporting, response and record-keeping in relation to online safety incidents
- To ensure compliance with safeguarding duties in KCSIE 2026, the Prevent Duty, and data protection laws (the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025)

3. Schedule for development, monitoring and review

- The implementation of this Online Safety Policy will be monitored by the Headteacher, Deputy Headteacher, Senior Leadership Team and Online Safety Lead
- Monitoring will take place at least once per annum
- The Local Governing Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at least once per annum
- The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety, or incidents that have taken place

Should serious online safety incidents take place, the following external persons/agencies should be informed: Steve Ellis (CEO, CAT); Luci Jones (Director of Operations); the Chair of Governors; CAT IT support ([*insert provider*]); the police (if required); and local safeguarding teams (if required).

[*Insert school name*] will monitor the impact of the policy using: logs of reported incidents; monitoring logs of internet activity (including sites visited) and filtering; internal monitoring data for network activity; surveys and questionnaires of pupils, parents and staff; and audit activity as required throughout the year, both to prevent and in response to any online safety incidents arising.

4. Roles and responsibilities

Local Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor in line with their role as Safeguarding Governor. The role of the Online Safety Governor includes: regular meetings with the Online Safety Lead; attendance at online safety group meetings; regular monitoring of online safety incident logs; regular monitoring of filtering and change control logs; and updates and reporting to relevant governors, board, committees and meetings.

In line with KCSIE 2026, the Governing Body ensures that a review of the effectiveness of filtering and monitoring systems is carried out **at least once every academic year**, undertaken by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT support, and that a record is kept of the checks made.

Headteacher and senior leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day-to-day responsibility for online safety will be delegated to the Online Safety Lead. The Headteacher and at least one other member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. The Headteacher and senior leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues as relevant.

The Headteacher and senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. These systems include: up-to-date acceptable use agreements for all pupils; up-to-date acceptable use agreements for all staff and volunteers; central records of reports of misuse of technology, including reports, investigations and outcomes; central records of monitoring logs of online safety incidents and appropriate actions arising; central records of staff training given in relation to online safety; and regular monitoring reports to the Senior Leadership Team from the Online Safety Lead.

SLT member responsible for filtering and monitoring

In line with KCSIE 2026, a named member of the SLT (*[insert name]*) is responsible for filtering and monitoring. They lead the annual review of filtering and monitoring effectiveness with the support of the DSL and IT support, ensure checks are carried out that filtering is working appropriately on all internet-connected devices in all relevant locations, keep a record of these checks, and ensure the leadership team and relevant staff understand the provisions in place and know how to escalate concerns.

Online Safety Lead

- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority, the Trust and other relevant bodies

- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety development
- meets regularly with the Online Safety Governor to discuss current issues and review incident logs and filtering/change control logs
- attends relevant meetings/committees of governors
- reports regularly to the Senior Leadership Team

Network manager / technical support

Mill View Primary School receives technical support through a formal service level agreement with Seven Eleven Systems Ltd. They are responsible for ensuring that: the school's technical infrastructure is secure and is not open to misuse or malicious attack; the school meets required online safety technical requirements and any Trust or Local Authority guidance that may apply; users may only access the networks and devices through a properly enforced password protection policy; the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person; they keep up to date with online safety technical information; the use of the network, internet, learning platform, remote access and email is regularly monitored so that any misuse or attempted misuse can be reported to the Headteacher, senior leaders or Online Safety Lead for investigation, action or sanction; and that monitoring software and systems are implemented and updated as agreed in school policies.

Teaching and support staff

Staff are responsible for ensuring that: they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices; they have read, understood and signed the Staff Acceptable Use Agreement (Appendix 1); they report any suspected misuse or problem to the Headteacher, senior leader or Online Safety Lead for investigation; all digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems; online safety issues are embedded in all aspects of the curriculum and other activities; pupils understand and follow the Online Safety Policy and acceptable use agreements; they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed); and, in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material found in internet searches.

Designated Safeguarding Lead

The DSL will be trained in online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from: the sharing of personal data; access to illegal or inappropriate materials; inappropriate online contact with adults or strangers (including AI applications that simulate such contact); potential or actual incidents of grooming; the making or sharing of nudes and semi-nudes (including AI-generated imagery); and online bullying. The DSL takes lead responsibility for safeguarding aspects of online safety, understands the filtering and monitoring systems in place and supports the annual review of their effectiveness.

Pupils

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement (see appendices)

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, including in relation to AI-generated content
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras, on the taking and use of images, and on online bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school, and realise that the school's Online Safety Policy covers their actions out of school if related to their membership of the school

Parents/carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the website and information about national and local online safety campaigns, including the DfE guidance for parents on children's screen time. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: digital and video images taken at school events; access to parents' sections of the website and online pupil records; and their children's personal devices in school (where this is allowed).

Community users

Where applicable, community users who access school systems as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems.

5. Online safety education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is an essential part of the school's safeguarding provision. Online safety is a focus across all areas of the curriculum, with staff reinforcing online safety messages wherever technology is used. The online safety curriculum is broad, relevant, progressive and age-appropriate. Education is provided in the following ways:

- A planned online safety curriculum, delivered through Kapow Computing and PSHE curriculum explicitly addressing all elements of the **4Cs of online safety** (content, contact, conduct, commerce)
- Key online safety messages reinforced through assemblies, pastoral activities and cross-curricular learning
- Pupils taught to be critically aware of the content they encounter online, including misinformation, disinformation, and AI-generated or manipulated material (e.g. deepfakes), and guided to validate the accuracy of information
- Pupils supported to acknowledge sources, respect copyright and understand digital ownership
- Pupils encouraged to build resilience to radicalisation by debating controversial issues in a safe environment and learning how to influence and participate in decision-making

- Pupils helped to understand and follow the Pupil Acceptable Use Agreements and to adopt safe and responsible behaviours both inside and outside of school
- Pupils made aware of the legal age limits for social networking sites and the risks and legal implications of posting online, including that all incidents involving the sharing of nude or semi-nude images require a safeguarding response, whether consensual or non-consensual
- KS1 pupils given supervised access to carefully selected, age-appropriate resources, with emphasis on asking for help and telling a trusted adult
- KS2 pupils supported to develop independence in safe use, including digital footprints, safe searching, reporting concerns and understanding online risks
- Staff modelling good practice in their own use of technology, the internet and mobile devices
- Internet use in lessons being pre-planned and directed to suitable sites; where free searching is permitted, staff remain vigilant in monitoring content and addressing issues that arise
- In exceptional cases where pupils need to research sensitive topics (e.g. racism, drugs, discrimination), temporary adjustments to filtering may be authorised by the Online Safety Lead or technical staff, with clear reasons recorded

Online safety education will be tailored where necessary to meet the needs of pupils with SEND, recognising that they may be more vulnerable to certain risks online. This approach ensures that online safety is embedded across the curriculum, supports the development of digital resilience and prepares pupils to use the digital world safely and responsibly.

Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, particularly within an ever-changing technological age. However, they play an essential role in the education of their children and in the monitoring and regulation of their children's online behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Mill View Primary School will therefore seek to provide information and awareness to parents and carers through: curriculum activities; letters, newsletters, the website and learning platform; parent/carer evenings and sessions; high-profile events and campaigns such as Safer Internet Day; and reference to relevant websites, publications and support materials, including the DfE guidance for parents on children's screen time.

Staff, governors and volunteers

It is essential that all staff, governors and volunteers receive regular online safety training and understand their responsibilities, as outlined in this policy. Training is provided in the following ways:

- **Annual training:** all staff receive safeguarding and online safety training every year (including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring), with additional updates during the year as required (e.g. to reflect new risks, statutory updates or local incidents)
- **Induction:** all new staff, governors and volunteers complete online safety and cyber security training as part of their induction before being given access to school systems, ensuring they fully understand the school's Online Safety Policy and acceptable use agreements
- **Governors:** governors receive updates on online safety as part of their safeguarding responsibilities, including how to interpret filtering and monitoring reports
- **Training needs audit:** the school carries out regular audits of training needs; central records of training are kept on staff files and in the online safety training log

- **Performance development:** where online safety is identified as a training need, appropriate training and support will be provided by the Online Safety Lead or external providers
- **Policy updates:** the Online Safety Policy and any updates are shared and discussed at staff meetings, INSET days and team briefings
- **Ongoing guidance:** the Online Safety Lead (or nominated person) provides targeted advice, guidance and training to individuals as required

This programme ensures that staff, governors and volunteers are confident in their role, aware of current and emerging online risks (including generative AI, misinformation and online scams), and able to promote safe, responsible and effective use of technology across the school community.

6. The four areas of online risk (the 4Cs)

The breadth of issues classified within online safety is considerable and ever-evolving, but can be categorised into four areas of risk, as set out in KCSIE 2026:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact:** being subjected to harmful online interaction with other users **or with generative AI applications that simulate this**; for example peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, **including those generated using AI**, and online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams; if pupils, students or staff are felt to be at risk, this can be reported to the Anti-Phishing Working Group

7. Safer use of technology

Mill View Primary School uses a wide range of technology to support learning, communication and administration, including computers, laptops, tablets and other digital devices; the internet, including search engines and educational websites; email systems; games-based and interactive learning technologies; and digital cameras, webcams and video recorders. All school-owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

To promote safe and effective use of technology: members of staff will always evaluate websites, tools and apps before use in the classroom or when recommending them for home learning; the use of internet-derived materials by staff and learners must comply with copyright law, with all sources acknowledged; and supervision of learners will always be appropriate to their age and ability.

Generative artificial intelligence (AI)

Where the school chooses to use generative AI (either teacher-facing or pupil-facing), we follow the DfE guidance **Generative Artificial Intelligence in Education** and the department's **Generative AI: product safety expectations**, which set out safety considerations, legal responsibilities and how filtering and monitoring requirements apply to the use of generative AI in education. Staff make use of the DfE's online AI training resources (developed with the Chiltern Learning Trust and the Chartered College of

Teaching), which include information on identifying and mitigating key risks associated with safeguarding, ethics, data protection and intellectual property. Pupils are taught, in an age-appropriate way, that AI can generate convincing but false or manipulated content, and that creating or sharing AI-generated nude or semi-nude imagery of any person under 18 is illegal and will be treated as a safeguarding matter.

8. Filtering and monitoring

In line with KCSIE 2026 and the DfE filtering and monitoring standards, the school ensures appropriate filtering and monitoring systems are in place and that a review of their effectiveness is carried out **at least once every academic year**. The review is carried out by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT support. It includes checks that filtering is working appropriately on **all internet-connected devices in all relevant locations**, and a record is kept of these checks. The school considers the number and age range of its children, those who are potentially at greater risk of harm, and how often they access the IT system, along with the proportionality of costs versus safeguarding risks.

- Mill View Primary School uses Sophos and monitoring systems *provided through Seven Eleven Systems Limited*.
- The school identifies and assigns roles and responsibilities to manage filtering and monitoring systems; the named SLT lead is Ali Gibbons.
- Filtering blocks harmful and inappropriate content, including extremist and terrorist content, without unreasonably impacting teaching and learning ('over-blocking')
- Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list; content lists are regularly updated and internet use is logged and regularly monitored
- Where changes to filters are requested, they are logged and kept on central record with reasons why the change was requested and the merit it held
- Logs are checked by the DSL/Online Safety Lead and reported to governors where appropriate
- The school uses the DfE's 'Plan technology for your school' service to self-assess against the filtering and monitoring standards where helpful, and refers to UK Safer Internet Centre and SWGfL guidance on appropriate filtering and monitoring

Devices

School-owned devices are provided for educational use only. Staff must not use personal devices to photograph or communicate with pupils.

Visitors

Visitors are required to follow safeguarding guidance and acceptable use terms. Where access is permitted (e.g. for contractors), this will be monitored and restricted to the purpose of their visit.

Images

Parent/carers consent must be obtained before publishing any pupil images. Pupil names will not be published alongside images. Images must only be captured and stored using school-owned devices, in line with safeguarding expectations.

9. Mobile phones

Pupils

In line with KCSIE 2026 and the DfE statutory guidance **Mobile Phones in Schools**, our school is a **mobile phone-free environment by default**; anything other than this is by exception only. Pupils do not have access to their mobile phones throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime. Pupils are discouraged from bringing mobile phones to school. Any who do, are required to turn them off at the school gate, hand them in at the main school office for the duration of the school day.

Staff use of personal devices and mobile phones

Staff must use personal devices in line with the law and school policies on confidentiality, safeguarding, data security and acceptable use. Staff must: keep personal devices stored securely (e.g. locked drawer/locker) and switched off or on silent during lessons; avoid using personal devices during teaching, unless authorised by the Headteacher in exceptional circumstances; only bring content onto site that is appropriate and consistent with their professional role; never use personal devices to contact pupils or parents/carers (any pre-existing relationships that may affect this rule must be discussed with the DSL and/or Headteacher); and never use personal devices to take or store photographs or videos of pupils - only school-provided equipment may be used for this purpose. Any breach of these expectations will be managed under the Staff Code of Conduct and Allegations Policy. Where there is reason to believe illegal content is stored or a criminal offence has been committed, the police will be contacted.

Visitors' use of personal devices

The safety and privacy of pupils is paramount. Parents, carers, volunteers and contractors must follow school safeguarding rules on personal device use. Visitors should not use personal devices on the premises unless it is essential for the purpose of their visit; leaders may request devices are left securely at the school office; safeguarding notices, signage and information will remind visitors of these expectations; visitors on site regularly or for extended periods must follow the school's Acceptable Use Policy and associated safeguarding policies; and staff are expected to challenge any inappropriate use of personal devices by visitors and report concerns immediately to the Headteacher/DSL (or deputy).

10. Data protection and security

The school complies with data protection laws: the Data Protection Act 2018, the UK GDPR and the Data (Use and Access) Act 2025. How [\[insert school name\]](#) conforms to the requirements of this legislation, and how this supports this Online Safety Policy, can be found within the Trust Data Protection Policy. [\[Insert school name\]](#) is responsible for ensuring that its IT systems, infrastructure and network are as safe and secure as reasonably possible and that the policies and procedures within this policy are fully implemented. In line with the updated information security expectations in KCSIE 2026, the school takes measures to safeguard its systems, data and users, including appropriate access management.

Access and permissions

Access to data is role-based: staff are only given access to the systems and files necessary for their work. Protected files and sensitive data are hidden from unauthorised users. Staff are not automatically granted access to the full management information system.

Passwords and devices

All users must use strong passwords and never share them. Devices that access school systems must be password-protected, locked when unattended and set to auto-lock after a short period of inactivity. Personal data must only be accessed on secure, school-managed devices; private equipment must not be used to store or access personal data.

Storage of data

Portable media (e.g. USB sticks) should only be used where absolutely necessary, and must always be encrypted and password protected. The preferred method of storing and sharing data is through the school's secure, cloud-based system (*[insert system, e.g. OneDrive]*), which provides encrypted services as standard. Staff must not share usernames or passwords; where documents are shared, this must be done through the approved sharing facility.

Secure transfer and remote access

Personal or sensitive data may only be removed from the school premises with the permission of the Headteacher and must always be encrypted, password protected and transported securely. Staff must ensure that personal devices or home computers are never used to access or store school personal data. Where school data is accessed remotely, secure log-in procedures must be used. All portable and mobile devices used to transmit or store school information must use approved encryption and security software. Failure to follow these rules may result in disciplinary action in line with the Staff Code of Conduct; serious breaches may be treated as a safeguarding or data protection incident and reported to the relevant authorities.

11. Social media and communications

Clear, professional and safe communication between staff, pupils and parents is vital to support learning and to safeguard the whole school community. All communication must comply with safeguarding, confidentiality, data protection and acceptable use policies.

Communication

- Staff must only use official school communication systems (e.g. school email, approved learning platforms) when contacting pupils, parents or carers; personal email, text messaging or social media must not be used
- All email and digital communications are monitored; staff should therefore ensure tone and content are always professional
- Any communication that makes a staff member feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature, must be reported immediately to the DSL/Online Safety Lead
- Pupils are taught about safe and respectful communication online, including the risks of sharing personal details and strategies for dealing with inappropriate contact
- Sensitive information must never be shared via unsecured channels; where necessary, approved secure systems (e.g. encrypted email) must be used

- Personal information about pupils, parents or staff must not be posted on the school website or shared outside secure school systems

Staff use of social media

Staff must maintain clear professional boundaries online. To protect both staff and the school, staff must not: refer to pupils, parents or colleagues on personal social media accounts; engage in online discussions about school-related matters on personal platforms; attribute personal opinions to the school or the Trust; connect with current or past pupils, or parents, on social media (except where a prior personal relationship exists); interact with school social media accounts from personal accounts; or post, like, comment on or share material that could be deemed offensive, discriminatory, inflammatory or damaging to the reputation of the school. Staff should regularly check privacy and security settings on personal accounts. Breaches of this guidance will be managed under the Staff Code of Conduct.

School use of social media

Mill View Primary School maintains official social media accounts to share information with the wider community. These are managed in line with safeguarding expectations and overseen by the Headteacher and Online Safety Lead. The school ensures that: accounts are checked regularly to ensure compliance with school policies; communication via social media is one-way, with comments and interactions restricted where possible; followers, comments, likes and other interactions are monitored and, where necessary, removed; at least two members of staff (including the Headteacher) are involved in the administration of school social media accounts; and clear systems are in place for reporting and addressing misuse or abuse of school social media platforms.

12. Reporting and responding to incidents

This guidance is for all staff when reporting or managing incidents involving the use of online services or technology. Online safety incidents may involve illegal or inappropriate activities, but may also arise from mistakes or misjudgements by otherwise well-intentioned users. All incidents must be taken seriously and handled in line with school safeguarding procedures.

- **Immediate action:** if there is any suspicion that a website, platform or device may contain child sexual abuse images, or if there is any other suspected illegal activity, this must be reported to the DSL immediately and referred to the police
- **Nudes and semi-nudes:** in line with KCSIE 2026, **all** incidents involving the making or sharing of nude or semi-nude images (including AI-generated images or 'deepfakes'), whether consensual or non-consensual, require a safeguarding response and must be reported to the DSL, who will follow the UKCIS guidance for education settings
- **Reporting process:** all concerns, whether involving staff, pupils, parents or visitors, must be reported promptly to the DSL (or deputy); incidents will be logged and acted upon in accordance with safeguarding procedures
- **Illegal activity:** any suspected criminal activity or illegal material will be referred without delay to the police and relevant external agencies
- **Child-centred approach:** pupils are encouraged to follow the "Stop, Block, Report" message and to seek help from a trusted adult whenever they encounter something online that worries them

- **Support:** staff will ensure that any child affected by an online safety incident receives appropriate support and guidance; where necessary, parents/carers will be informed and external agencies engaged

This structured approach ensures that all online safety incidents are managed consistently, proportionately and with the protection of children at the centre.

13. Sanctions

At Mill View Primary School, most online safety incidents are expected to involve inappropriate rather than illegal misuse of technology. It is important that such incidents are addressed quickly, proportionately and consistently, so that members of the school community understand expectations and trust that concerns are dealt with.

- **Proportionate response:** all incidents of deliberate misuse of technology, in breach of this Online Safety Policy or associated acceptable use agreements, will be addressed in line with the school's Behaviour Policy (for pupils) or Staff Code of Conduct (for staff)
- **Escalation:** repeated or serious misuse may result in restricted access to technology, parental involvement, formal disciplinary action, or referral to external agencies where necessary
- **Transparency:** where appropriate, staff and pupils will be made aware that incidents have been dealt with, to reinforce understanding of safe and responsible behaviour
- **Illegal misuse:** where misuse involves illegal activity, this will be treated as a safeguarding or criminal matter and referred to the police or relevant authorities immediately

14. Technical infrastructure

Mill View Primary School is responsible for ensuring that the school infrastructure and network are as safe and secure as is reasonably possible and that the policies and procedures approved within this policy are implemented. Working with Seven Eleven Systems the school ensures that:

- School technical systems are managed in ways that ensure the school meets recommended technical requirements
- There are regular reviews and audits of the safety and security of school technical systems
- All users have clearly defined access rights to school technical systems and devices
- All users (at KS2 and above) are provided with a username and secure password by the school, which keeps an up-to-date record of users and their usernames
- The 'master/administrator' passwords for the school ICT systems, used by the network manager, are also available to the Headteacher or another nominated senior leader and kept in a secure place
- Office staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks reconcile licences purchased against installations
- Internet access is filtered for all users and filtering/monitoring ensures that children are safe from terrorist and extremist material when accessing the internet
- School technical staff regularly monitor and record the activity of users on the school technical systems, and users are made aware of this in the acceptable use agreements
- An appropriate system is in place (reporting to the Online Safety Lead) for users to report any actual or potential technical incident or security breach
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations and mobile devices from accidental or malicious attempts to threaten the

security of school systems and data; these are tested regularly, and the school infrastructure and individual workstations are protected by up-to-date anti-virus software

- In the event that any personal device is allowed to be connected to the school network, users abide by the acceptable use policy and the terms detailed within it

Appendix 1: Staff and Volunteer Acceptable Use Agreement

Staff / volunteer name: _____ Signed: _____ Date: _____

Purpose

Digital technologies are integral to education and professional life. They support learning, creativity, communication and school operations. With these opportunities come responsibilities: all staff and volunteers must use technology safely, lawfully and professionally to protect themselves, pupils, colleagues and Mill View Primary School. This agreement ensures that staff and volunteers act as responsible users who safeguard themselves and others; school systems and data are protected from misuse or security risks; and staff are clear about professional boundaries when using technology, including generative AI tools.

Professional and personal safety

- I understand the school monitors my use of digital technology and communications systems
- I will use school systems primarily for educational purposes; limited personal use may be permitted in line with school policy
- I will keep my username and password secure and never share them
- I will immediately report illegal, inappropriate or harmful content or incidents to the DSL or Headteacher

Professional conduct online

- I will communicate professionally at all times, avoiding offensive or inappropriate language
- I will not access, copy or alter other users' files without permission
- I will only take and publish images in line with school policy, using school equipment (not personal devices) and with appropriate consent
- I will only communicate with pupils and parents/carers through official school systems
- I will not engage in online activity that compromises my professional role
- I will only use generative AI tools in line with school and Trust guidance, and never enter personal data about pupils, parents or staff into AI tools that have not been approved by the school

Use of devices and data

- When using mobile devices or personal equipment in school, I will follow the same rules as for school-owned devices; devices must be secure, virus-protected and password-protected
- I will not use personal email accounts for school business
- I will not install unauthorised software or attempt to bypass school security systems
- I will not access or download illegal or harmful materials
- I will handle personal data securely and in line with school policy and data protection laws, ensuring digital data is encrypted and paper records are stored safely
- I will report any equipment faults or damage immediately

Copyright and fair use

- I will respect copyright and only use the original work of others with permission
- I will not distribute copyrighted material without authorisation

Responsibilities beyond school

This agreement applies to my use of school systems both in and out of school, and to my use of personal devices in any school-related context. I understand that breaches may result in disciplinary action, which could include warnings, suspension, referral to the governing body, or police involvement if illegal activity is suspected.

Declaration

I have read and understood this agreement. I agree to use school digital systems (in and out of school) and any personal devices used for school purposes responsibly, safely, and in line with this policy.

Appendix 2: KS1 (Infant) Pupil Acceptable Use Agreement

This is how we stay safe when we use computers, tablets and the internet:

- I will ask a teacher or another trusted adult if I want to use the computer or tablet
- I will only use the activities that my teacher or adult says I can use
- I will look after the computer, tablet and other equipment carefully
- I will not talk to people online unless a teacher or trusted adult is with me
- I will ask for help if I am not sure what to do, or if I think I have done something wrong
- I will tell a teacher or trusted adult straight away if I see something that upsets or worries me
- I know that if I do not follow these rules, I might not be allowed to use the computer or tablet

Appendix 3: KS2 Pupil Acceptable Use Agreement

Digital technology is an important part of life and learning. At *[insert school name]*, we want you to enjoy using computers, tablets and the internet safely, responsibly and respectfully. This agreement helps keep everyone safe and makes sure our school systems are used properly.

Keeping myself safe

- I know the school may check my use of computers, devices and online activity
- I will keep my username and password private and never use someone else's
- I will not share personal information online (like my name, address, phone number, school or passwords)
- I will be careful when talking to people online, and remember that some 'people' online might not be real people at all
- I will tell a teacher or trusted adult straight away if I see or receive anything online that upsets me

Respecting others

- I will use school systems for learning and not for games, shopping or sharing files unless a teacher allows it
- I will be polite and respectful online; I will not use unkind, aggressive or rude language
- I will not take or share photos, videos or recordings of anyone without permission

Using technology responsibly

- I will only use my own devices (like phones, USB sticks or cameras) in school if a teacher gives me permission
- I will not try to look at or download anything illegal, harmful or inappropriate
- I will not try to get around the school's filters or change computer settings
- I will not open email links or attachments unless I trust the sender
- I will look after school equipment and report any damage or faults immediately

Research and learning online

- I will check that information I find online is accurate, as not everything is true - including pictures and videos that can be made or changed by computers (AI)
- I will respect other people's work and copyright; I won't copy or share work, music or videos without permission

Taking responsibility

- I understand this agreement applies in school, when using school systems at home, and when I use my own devices in ways that link to school (e.g. communicating with classmates)
- I understand the school can take action if I am involved in online bullying or other inappropriate behaviour, even if it happens out of school
- I know that breaking these rules may mean I lose access to school systems and my parents/carers will be told; serious incidents may lead to further consequences

Signed (pupil): _____ **Date:** _____