



Acceptable Use Policy (AUP)

2026-27

Our Mission

'At SS John and Monica's we learn through the example of Jesus to love, respect, understand and value each other'

Contents

1. Introduction and aims	3
2. Relevant legislation and guidance	3
3. Definitions.....	4
4. Unacceptable use	5
5. Staff (including governors, volunteers, and contractors)	7
6. Pupils.....	12
7. Parents/carers	14
8. Data security	15
9. Protection from cyber attacks.....	18
10. Internet access	19
11. Monitoring and review	20
12. Related policies	20
Appendix 1 – Acceptable Use Agreement for Parents and Carers	22
Appendix 2 – Acceptable Use Agreement for KS2 Pupils.....	23
Appendix 3 – Acceptable Use Agreement for Younger Pupils	24
Appendix 4 – Acceptable Use Agreement for Adults	25

1. Introduction and aims

Information and communications technology (ICT) and digital technology are an integral part of the way our school works and are important resources for pupils, staff (including the senior leadership team), governors, volunteers, contractors and visitors. They support teaching and learning, communication, administration and the wider work of the school.

However, the use of technology and online services can also present risks relating to safeguarding, online safety, data protection, cyber security and the wellbeing of children and adults.

Online safety is an integral part of safeguarding at SS John & Monica Catholic Primary School. In line with our school Mission, we aim to enable pupils to benefit from technology while developing the knowledge, skills and behaviours needed to use it safely, responsibly, respectfully and critically.

This policy aims to:

- Set clear expectations and rules for the safe and appropriate use of the school's ICT systems, devices, networks and online services by staff, pupils, parents/carers, governors, volunteers, contractors and visitors.
- Establish clear expectations for how members of the school community communicate and behave online.
- Protect children from potentially harmful and inappropriate online material and activity.
- Support the school's safeguarding, child protection, data protection, behaviour and cyber security arrangements.
- Ensure that appropriate filtering and monitoring systems are in place and that staff understand their responsibilities for online safety.
- Support pupils to recognise, assess and manage online risks and to know how and where to seek help.
- Promote responsible, respectful and critical use of digital technology, including emerging technologies and artificial intelligence (AI).
- Protect the confidentiality, integrity and security of school information, systems and personal data.
- Prevent disruption or harm arising from the misuse, or attempted misuse, of the school's ICT systems and digital technology.
- Support the school in providing a planned and progressive approach to online safety education.

This policy applies to all users of the school's ICT facilities and digital services, including governors, staff, pupils, volunteers, contractors and visitors. It applies to the use of school-owned devices and systems both on and off the school premises and, where relevant to safeguarding, behaviour or the reputation of the school, to the use of personal devices and online services.

Breaches of this policy will be addressed in accordance with the school's relevant policies and procedures, including the Behaviour and Relationships Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct and Data Protection Policy.

2. Relevant legislation and guidance

This policy has due regard to all relevant legislation, statutory guidance and national standards, including, but not limited to:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)

- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Education Act 2011
- Education and Inspections Act 2006
- Education and Training (Welfare of Children) Act 2021
- Online Safety Act 2023
- [Keeping Children Safe in Education 2026](#)
- [Prevent Duty Guidance: England and Wales](#)
- [DfE – Searching, Screening and Confiscation in Schools](#)
- [DfE – Mobile Phones in Schools](#)
- [DfE – Meeting Digital and Technology Standards in Schools and Colleges](#)
- [DfE – Filtering and Monitoring: Core Standard](#)
- [DfE – Cyber Security: Core Standard](#)
- [DfE – Generative Artificial Intelligence \(AI\) in Education](#)
- [DfE – Generative AI Product Safety Standards](#)
- [DfE – Data Protection in Schools](#)
- [National Cyber Security Centre \(NCSC\) – Cyber Security for Schools](#)
- [UK Council for Internet Safety \(UKCIS\) – Sharing Nudes and Semi-Nudes: Advice for Education Settings](#)

The school will have regard to any subsequent updates or replacements to the legislation, statutory guidance and national standards referenced within this policy.

Related school policies and documents

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Behaviour and Relationships Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Artificial Intelligence (AI) Use Policy
- Mobile Phone and Smart Devices Policy
- Acceptable Use Agreements
- Online Safety and Digital Responsibility Whole School Overview
- relevant curriculum and safeguarding guidance relating to online safety.

3. Definitions

For the purposes of this policy:

- **ICT and digital technology** includes all computing and communication equipment, systems and services used by or on behalf of the school. This includes computers, laptops, tablets, networks, internet access, email, cloud-based services, software, applications and other digital platforms.

- **School ICT facilities and systems** includes any device, network, system, software, application, account or online service owned, provided, managed or authorised by the school.
- **Personal devices** includes personally owned mobile phones, smartphones, tablets, laptops, smartwatches, wearable technology and other internet-enabled or communication devices. Pupil use of these devices is governed by the school's **Mobile Phone and Smart Devices Policy**.
- **Online safety** refers to safeguarding individuals when using digital technology and online services. This includes protecting children from harmful or inappropriate content, contact, conduct and online commercial risks, and supporting them to use technology safely, responsibly and critically.
- **Filtering** refers to the systems used by the school to restrict access to inappropriate, harmful or illegal online content.
- **Monitoring** refers to the systems and processes used by the school to identify potentially concerning or inappropriate activity on school devices, networks and systems so that appropriate safeguarding or other action can be taken.
- **Artificial intelligence (AI)** refers to digital systems capable of performing tasks commonly associated with human intelligence. **Generative AI** refers to systems capable of creating content such as text, images, audio or other material in response to user prompts. The use of AI within school is governed by the school's **Artificial Intelligence (AI) Use Policy**.
- **Cyber security** refers to the measures taken to protect the school's devices, networks, systems, accounts and data from unauthorised access, loss, damage, disruption or cyber attack.
- **Users** means anyone authorised to use, or who has access to, the school's ICT facilities, systems or digital services, including pupils, staff, governors, volunteers, contractors and visitors.

4. Unacceptable use

The school expects all users of its ICT facilities, systems and digital services to use technology safely, responsibly, respectfully and lawfully.

The following uses of the school's ICT facilities, systems, networks and digital services are considered unacceptable and are prohibited unless specifically authorised for a legitimate educational, safeguarding or administrative purpose:

- Accessing, creating, downloading, storing, sharing or distributing illegal, inappropriate, harmful, offensive or explicit material.
- Accessing, creating or sharing content that is discriminatory, racist, sexist, homophobic, transphobic, extremist, antisemitic or otherwise promotes hatred or intolerance.
- Using technology to bully, harass, threaten, intimidate, abuse or discriminate against another person, including through social media, messaging, online games or other digital platforms.
- Creating, requesting, possessing, sharing or distributing nude or semi-nude images or videos of children or young people, including AI-generated or digitally manipulated material. Any safeguarding concerns of this nature will be managed in accordance with the school's Safeguarding and Child Protection Policy and current UKCIS guidance.
- Accessing or distributing pornographic, excessively violent or other age-inappropriate content.
- Using school systems for gambling, scams, phishing, fraud or other unlawful or dishonest activity.
- Attempting to bypass, disable, interfere with or circumvent the school's filtering, monitoring, security or access-control systems.
- Attempting to gain unauthorised access to accounts, devices, networks, systems or data, or deliberately introducing malware, viruses or other malicious software.

- Sharing passwords or login credentials, using another person's account, or allowing another person to use an account without authorisation.
- Disclosing, uploading or sharing confidential, personal or sensitive information without appropriate authority.
- Using unauthorised software, applications, online services, devices or removable storage on school systems where permission is required.
- Using school ICT facilities for unauthorised commercial activity, private business or personal financial gain.
- Infringing copyright, intellectual property rights or software licensing arrangements.
- Recording, photographing, livestreaming or sharing images, audio or video of pupils, staff or others without appropriate permission or a legitimate school purpose.
- Using social media, messaging services, online communities or communication platforms in a way that breaches school policies, compromises professional boundaries, causes harm or brings the school into disrepute.
- Using artificial intelligence or generative AI in a way that breaches the school's **Artificial Intelligence (AI) Use Policy**, including entering personal, confidential, sensitive or safeguarding information into unauthorised AI systems or using AI to circumvent learning or professional responsibilities.
- Using personal mobile phones, smartwatches or other smart devices contrary to the school's **Mobile Phone and Smart Devices Policy**.
- Deliberately damaging, disrupting or misusing school devices, networks, systems, data or digital services.
- Any other use that may compromise safeguarding, data protection, cyber security, the effective operation of the school or the safety and wellbeing of members of the school community.

Any suspected safeguarding concern arising from the use of technology must be reported immediately in accordance with the school's safeguarding procedures. Cyber security incidents, suspected data breaches, phishing attempts or unauthorised access must be reported promptly to the appropriate member of staff in accordance with school procedures.

Breaches of this policy may result in access to school ICT facilities or systems being restricted or withdrawn and may be addressed through the school's Behaviour and Relationships Policy, Staff Code of Conduct, disciplinary procedures or other relevant policies. Where appropriate, concerns may also be reported to parents/carers, the local authority, police or other relevant agencies

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities, systems or digital services (on the school premises and/or remotely) is required for a legitimate educational, safeguarding, administrative or technical purpose that would otherwise be considered unacceptable use under this policy, an exception may be granted at the discretion of the headteacher or other appropriately authorised personnel.

This may include **authorised testing of the school's filtering and monitoring systems**, where designated staff deliberately attempt to access or search for content that would ordinarily be prohibited in order to check that filtering, monitoring and safeguarding systems are operating effectively.

Any such activity must have a legitimate school purpose, be carried out only by appropriately authorised personnel and be necessary and proportionate. It must not unnecessarily expose pupils or other staff to harmful content or compromise safeguarding, data protection or cyber security.

Where an exception relates to the use of artificial intelligence (AI) or generative AI, this must be in accordance with the school's **Artificial Intelligence (AI) Use Policy**.

4.2 Sanctions

Pupils, staff and other users who engage in unacceptable use of the school's ICT facilities, systems or digital services may be subject to appropriate action in line with the school's relevant policies and procedures.

For pupils, this may include consequences in accordance with the school's **Behaviour and Relationships Policy**, together with additional safeguarding or pastoral action where appropriate.

For staff, governors, volunteers and contractors, concerns may be addressed through the **Staff Code of Conduct**, disciplinary procedures, safeguarding procedures or contractual arrangements, as appropriate.

Depending on the nature and seriousness of the incident, the school may:

- restrict, suspend or withdraw access to ICT facilities, systems, accounts or devices
- confiscate devices where permitted and appropriate
- inform parents or carers
- record and respond to safeguarding concerns in accordance with the school's safeguarding procedures
- investigate possible data protection or cyber security incidents
- refer concerns to the local authority, police, social care, the LADO or other relevant agencies where required.

Any response will be proportionate to the nature of the incident and will take account of safeguarding, the age and needs of the individual, and whether the incident indicates that a child may be at risk of harm or exploitation.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

Access to the school's ICT facilities, systems, accounts and digital services is managed by authorised ICT personnel in accordance with the user's role and responsibilities.

This includes, but is not limited to:

- computers, laptops, tablets and other school-owned devices
- school networks and internet access
- email and cloud-based services
- software, applications and online platforms
- access permissions for particular systems, folders, files or data.

Staff and other authorised users will be provided with individual login and account credentials where appropriate. Users must not share passwords, accounts or authentication details with others and must take reasonable steps to keep them secure.

Access permissions should be appropriate to the individual's role. Where a member of staff has access to information, files, systems or functions that they do not believe they are authorised to access, they must report this promptly to the ICT manager or another appropriate senior member of staff. Changes to access permissions must be authorised and implemented appropriately.

Users must not attempt to gain additional access privileges, access another person's account or circumvent security, filtering or monitoring arrangements unless specifically authorised for a legitimate purpose in accordance with **section 4.1** of this policy.

Staff must only use school-approved systems, applications and online services for storing or processing school information and personal data. The use of artificial intelligence tools must be in accordance with the school's **Artificial Intelligence (AI) Use Policy**.

All staff, governors, volunteers, contractors and other users granted access to school ICT systems must be made aware of the school's acceptable-use expectations appropriate to their role. **The school will obtain and retain appropriate evidence, at least annually, that relevant users have read, understood and agreed to comply with the school's Acceptable Use Policy/Agreement.**

Access to systems and accounts will be reviewed and removed or amended when it is no longer required, including when a user changes role or leaves the school.

5.1.1 Use of phones and email

The school provides staff with a school email account for work-related communication.

School email accounts must be used for school business. Staff must not use personal email accounts to send or receive work-related information, particularly where this includes personal, confidential, sensitive or safeguarding information.

Multi-factor authentication must be enabled where available.

Staff must:

- keep account credentials secure and must not share passwords or authentication codes
- check recipients carefully before sending emails, particularly where personal or confidential information is included
- use appropriate security measures when sharing sensitive or confidential information
- report suspected phishing, malicious emails, compromised accounts or other cyber security concerns promptly
- avoid opening unexpected links or attachments where their legitimacy is uncertain
- use professional, respectful and appropriate language in all electronic communications
- be mindful that school emails and other electronic communications may be retained, monitored and disclosed where required by law.

If a member of staff receives an email or information in error, they must not use or disclose that information. They should inform the sender and delete the information as appropriate.

If a member of staff sends personal, confidential or sensitive information to an unintended recipient, or suspects that a data breach has occurred, this must be reported **immediately to the Headteacher/DDSL and in accordance with the school's Data Protection Policy and data breach procedures**.

Staff must not normally provide their personal telephone numbers or personal contact details to pupils or parents/carers. Work-related communication with families should take place through school-approved communication systems and devices.

Where staff use school telephones, mobile devices or other communication systems, these must be used appropriately and in accordance with this policy, the **Staff Code of Conduct, Data Protection Policy** and any other relevant school procedures.

Personal mobile phones and smart devices must be used in accordance with the school's expectations for staff and must not be used in a way that compromises safeguarding, confidentiality, professional boundaries or the supervision of pupils.

5.2 Personal use

Staff may make limited personal use of the school's ICT facilities and systems where this does not interfere with their professional duties, the learning or supervision of pupils, or the effective operation of the school.

Personal use must:

- not constitute unacceptable use as defined in section 4 of this policy
- not take place when it would distract from professional responsibilities or the supervision of pupils
- not involve storing inappropriate, excessive or non-work-related material on school systems or devices
- not compromise safeguarding, confidentiality, data protection, cyber security or professional standards
- not make use of school systems for unauthorised commercial activity or personal financial gain.

Staff should be aware that use of school ICT facilities and systems may be subject to the school's filtering, monitoring and security arrangements, including where limited personal use is permitted.

Personal devices, including mobile phones and smart devices, may only be used in accordance with the school's **Staff Code of Conduct, Mobile Phone and Smart Devices Policy** and other relevant school expectations. Their use must not compromise safeguarding, confidentiality, professional boundaries or the supervision of pupils.

Staff must not use personal devices, personal accounts or personal cloud storage to store or process school information, personal data, safeguarding information or other confidential material unless specifically authorised and appropriately secured.

Staff should also be mindful that personal online activity, including social media use outside working hours, may have professional implications where it affects safeguarding, professional boundaries, confidentiality, the reputation of the school or confidence in their role.

5.2.1 Personal social media accounts

Staff must ensure that their use of social media, messaging services and other online platforms, whether for work or personal purposes, is appropriate and consistent with their professional responsibilities.

Staff must:

- maintain appropriate professional boundaries with pupils and parents/carers and must not use personal social media accounts to communicate with pupils
- use appropriate privacy and security settings and regularly review these
- not share confidential, personal or safeguarding information relating to pupils, families, staff or the school
- not post or share photographs, videos or other information relating to pupils unless through an authorised school account and in accordance with the school's consent and data protection arrangements
- not post, share or engage with content that could compromise safeguarding, professional standards, confidentiality or the reputation of the school
- not use social media to discuss individual pupils, parents/carers, colleagues or confidential school matters
- report any online contact, communication or activity involving a pupil that causes a safeguarding or professional-boundary concern in accordance with the school's safeguarding procedures.

Staff should be mindful that privacy settings do not guarantee that information posted online will remain private. Content may be copied, shared, screenshotted or otherwise distributed beyond its intended audience.

Any concerns regarding inappropriate online contact between a member of staff and a pupil, or concerns about staff conduct online, must be reported in accordance with the school's **Safeguarding and Child Protection Policy, Staff Code of Conduct** and procedures for managing allegations and low-level concerns.

5.3 Remote access

Where authorised, staff may access school systems, services and information remotely using **school-approved methods of remote access, including the school's secure Virtual Private Network (VPN)**.

Staff accessing school systems remotely must follow the same safeguarding, acceptable use, data protection and cyber security requirements that apply when working on school premises.

Staff must:

- use only authorised accounts and secure methods of remote access
- keep passwords and authentication details secure and use multi-factor authentication where available
- take reasonable precautions to prevent unauthorised persons from viewing or accessing school information
- ensure school devices are kept physically secure and are not left unattended in locations where they could be accessed by others
- not download or store personal, confidential or safeguarding information on personal devices or personal cloud-storage services
- report lost or stolen devices, suspected account compromise, malware, phishing or other security incidents promptly.

School information accessed remotely must be handled in accordance with the school's **Data Protection Policy, Safeguarding and Child Protection Policy** and relevant cyber security procedures.

The use of AI tools when working remotely remains subject to the school's **Artificial Intelligence (AI) Use Policy**.

5.4 School social media accounts

The school may operate official social media accounts and other online communication channels. These accounts may only be accessed, managed or used to publish content by members of staff who have been authorised to do so by the Headteacher.

Staff who are authorised to manage or post to school accounts must ensure that:

- content is appropriate, professional and consistent with the values and expectations of the school
- personal, confidential or safeguarding information is not shared
- photographs, videos or information relating to pupils are only shared where appropriate consent and permissions are in place
- school accounts are kept secure and login details are only available to authorised users
- any inappropriate comments, messages, contact or safeguarding concerns arising through a school account are reported promptly in accordance with the school's safeguarding procedures
- school accounts are not used for personal purposes.

Staff must not create social media accounts, groups or other online channels representing the school without appropriate authorisation.

Use of school social media and online communication channels must comply with the school's **Safeguarding and Child Protection Policy, Data Protection Policy, Staff Code of Conduct** and this policy.

5.5 Monitoring and filtering of the school network and use of ICT facilities

Filtering and monitoring are an important part of the school's safeguarding arrangements. The school maintains appropriate filtering and monitoring systems to help protect pupils and staff from illegal, inappropriate and potentially harmful online content and activity.

Filtering and monitoring arrangements apply, where technically appropriate, to users accessing the school network and to school-managed devices. The school recognises that no filtering or monitoring system can be completely effective and that technical systems do not replace effective supervision, education and professional vigilance.

Staff responsibilities

All staff must understand their role in relation to filtering and monitoring. When pupils are using devices, staff must maintain appropriate **in-person supervision and awareness of how devices are being used**, alongside the school's technical monitoring arrangements.

Staff must report promptly where:

- unsuitable or harmful material has been accessed or can be accessed
- filtering or monitoring appears not to be working effectively
- pupils attempt to bypass filtering or monitoring controls
- unusual or concerning online activity is identified
- filtering is unreasonably restricting legitimate teaching and learning
- there is any other online safeguarding or technical concern.

Safeguarding concerns must be reported to the **Designated Safeguarding Lead (DSL) or a Deputy DSL** in accordance with the school's safeguarding procedures. Technical concerns should also be reported to the appropriate ICT support.

Roles and oversight

The Governing Body has overall strategic responsibility for ensuring that appropriate filtering and monitoring arrangements are in place and that the school meets the Department for Education's Filtering and Monitoring Standards.

The DSL takes lead responsibility for safeguarding and online safety in relation to filtering and monitoring and works with senior leaders and the school's ICT support provider to review reports, respond to concerns and ensure appropriate action is taken.

ICT support is responsible for the technical maintenance and effective operation of the filtering and monitoring systems and for providing appropriate reports and information to the school.

Checking and reviewing effectiveness

The effectiveness of filtering and monitoring provision will be reviewed **at least annually**, and additionally following significant safeguarding concerns, changes to technology or systems, or where there is reason to believe that existing arrangements may not be effective.

Appropriate checks will be carried out and recorded to establish that filtering and monitoring arrangements are operating effectively. These checks will include, where appropriate, different user profiles, including **pupil and staff access, and different school-managed devices**.

Where practicable, pupils use individually identifiable accounts and devices so that online activity can be attributed to the appropriate user. Pupils are provided with individual login credentials when accessing school laptops and other compatible devices. Classroom iPads are allocated to individual pupils for use, enabling activity to be traced to the pupil using the device.

Staff must ensure that pupils use their allocated device or individual account and must not knowingly allow pupils to use another pupil's account or allocated device.

Checks and reviews will consider emerging risks and technologies, including **generative AI and dynamically generated online content**.

The school will maintain appropriate records of filtering and monitoring checks, concerns, incidents and resulting actions. Significant safeguarding concerns or weaknesses identified through filtering and monitoring will be shared with the DSL, senior leaders, ICT support and governors as appropriate.

The responsible governor will receive appropriate information to provide assurance that the Department for Education's Filtering and Monitoring Standards are being met. This will include opportunities, where appropriate, to scrutinise evidence and test the effectiveness of arrangements during monitoring visits.

Any authorised testing of filtering and monitoring systems involving potentially inappropriate search terms or content must be carried out in a controlled manner by, or with the approval of, appropriate senior leaders/ICT support and in accordance with section 4.1 of this policy.

Filtering and monitoring arrangements will be considered as part of the school's wider annual review of online safety provision, with identified actions recorded and monitored.

6. Pupils

6.1 Access to ICT facilities

Pupils are provided with access to school ICT facilities, devices, online services and the internet for educational purposes and other activities authorised by the school.

Pupils must use school technology in accordance with this policy and the age-appropriate **Acceptable Use Agreement**.

Pupils will normally access school ICT facilities under the supervision and direction of staff. Staff will maintain appropriate in-person supervision when pupils are using technology, alongside the school's technical filtering and monitoring arrangements.

Where individual pupil accounts are available, pupils will be provided with their own login credentials. Pupils must use their own account and must not share passwords, use another pupil's account or attempt to access another user's files or information.

Classroom iPads are allocated to individual pupils for use wherever practicable. Pupils should use their allocated iPad and must not swap or use another pupil's allocated device without permission from a member of staff. This supports the school in identifying and monitoring activity associated with individual users.

Pupils must not attempt to disable, circumvent or bypass the school's security, filtering or monitoring systems.

Pupils are taught to report anything they encounter online that makes them feel worried, uncomfortable or unsafe, or that they believe may be inappropriate. Concerns should be reported to a trusted adult in school as soon as possible.

Access to AI tools by pupils must be **teacher-directed, age-appropriate and in accordance with the school's Artificial Intelligence (AI) Use Policy**.

The school may restrict or withdraw access to ICT facilities where they are misused, alongside any action taken in accordance with the school's Behaviour Policy and safeguarding procedures.

6.2 Search and deletion

The Headteacher and members of staff authorised by the Headteacher may search pupils and their possessions, and confiscate electronic devices, where permitted by law and in accordance with current Department for Education **Searching, Screening and Confiscation** guidance, the school's **Behaviour Policy, Mobile Phone and Smart Devices Policy** and safeguarding procedures.

Where there are reasonable grounds to suspect that an electronic device contains data or material that has been, or could be, used to cause harm, disrupt teaching, break school rules or commit an offence, authorised staff may examine data or files on the device where legally permitted to do so.

Any search or examination of an electronic device must be necessary, proportionate and undertaken with due regard to the pupil's safeguarding, privacy and individual circumstances.

Where a search or confiscation gives rise to a safeguarding concern, the **Designated Safeguarding Lead (DSL) or a Deputy DSL must be informed immediately** and the school's safeguarding procedures followed.

Where there is any concern that a device contains nude or semi-nude imagery of a child, staff must not intentionally view, copy, print, share, store, save or delete the imagery, nor ask a pupil to show, share, download or delete it. The device should be secured and the concern reported immediately to the DSL or a Deputy DSL. The DSL/DDSL will follow current UKCIS guidance and determine the appropriate safeguarding response, including referral to the police and/or children's social care where appropriate.

If a member of staff inadvertently sees such imagery, for example because a pupil shows it to them before they can prevent this, they must not investigate further or continue viewing it. They must report this immediately to the DSL/DDSL and record the circumstances in accordance with the school's safeguarding procedures.

Where there is reason to believe that an electronic device contains evidence of a criminal offence or material requiring police involvement, staff should avoid taking action that could compromise that evidence. Where appropriate, the device will be secured and passed to the police. UKCIS advises that where a device needs to be passed to police, it should be disconnected from Wi-Fi/data, switched off and securely stored pending collection.

Where material does not raise a safeguarding or criminal concern, authorised staff may delete data or files where legally permitted and appropriate to do so.

Searches, confiscations and decisions relating to electronic devices will be recorded where appropriate in accordance with the school's behaviour and safeguarding procedures. Parents/carers will be informed where required or appropriate.

6.3 Unacceptable use of ICT and the internet outside school

The school recognises that pupils' use of technology outside school can affect the safety, wellbeing and education of pupils within school.

The school may respond to online behaviour that takes place outside school where it:

- poses a safeguarding risk to a pupil or another person
- involves bullying, harassment, discrimination, threats or harmful sexual behaviour
- involves the sharing of inappropriate, harmful or illegal content
- adversely affects another pupil's ability to feel safe or learn at school
- disrupts the orderly running of the school
- damages the reputation of the school or members of the school community.

Where such behaviour comes to the school's attention, it will be considered in accordance with the school's **Behaviour Policy, Anti-Bullying Policy and Safeguarding and Child Protection Policy**.

Safeguarding concerns arising from pupils' online activity outside school must be reported to the **DSL or a Deputy DSL** and appropriate safeguarding procedures followed. Where necessary, the school will work with parents/carers and relevant external agencies, including children's social care and the police.

Pupils are encouraged to report online incidents or concerns to a trusted adult, regardless of whether the incident occurred in school or at home

7. Parents/carers

Parents and carers play an important role in supporting children to use technology safely and responsibly. The school will work in partnership with families to promote consistent online safety messages between school and home.

Parents and carers are expected to:

- support their child in following the school's **Acceptable Use Agreement** and expectations for safe and responsible use of technology
- encourage their child to report anything online that worries, upsets or makes them feel unsafe
- raise concerns about online safety with the school promptly where these may affect their child or another member of the school community
- communicate respectfully when using school communication systems, social media or other online platforms
- respect the privacy of pupils, staff and families, including when sharing photographs, videos or information online
- support the school's expectations regarding mobile phones and smart devices.

The school will provide parents and carers with information and guidance to help them support their children online. This will include information about emerging online risks, age-appropriate use of technology, social media, online relationships, cyberbullying, scams, misinformation and the safe and responsible use of artificial intelligence.

Parents and carers will be informed that the school uses **filtering and monitoring systems** to help safeguard pupils when using school networks and devices. The school recognises that technical systems cannot remove all online risk and works alongside education, supervision and appropriate safeguarding procedures.

The school will provide clear routes through which parents and carers can report online safety or safeguarding concerns. Where a concern relates to the safety or welfare of a child, it will be dealt with in accordance with the school's **Safeguarding and Child Protection Policy**.

Parents and carers will be asked to acknowledge the school's acceptable-use expectations as appropriate.

7.1 Access to ICT facilities and materials

Parents and carers do not normally have access to the school's ICT facilities, systems or accounts.

Where access to a school device, system, online platform or network is provided for a specific purpose, parents and carers must follow the school's acceptable-use, safeguarding, data protection and security requirements.

Login details or access credentials provided by the school must be kept secure and must not be shared with unauthorised individuals.

Parents and carers must not attempt to access accounts, systems, files or information for which they have not been authorised, or attempt to bypass the school's security, filtering or monitoring arrangements.

Any suspected security issue, unauthorised access or accidental access to information should be reported to the school promptly.

7.2 Communicating with or about the school online

The school recognises the important role parents and carers play in modelling respectful and responsible online behaviour for children.

When communicating with the school, or discussing matters relating to the school through social media, messaging services, online groups or other digital platforms, parents and carers are expected to:

- communicate respectfully about pupils, staff and other members of the school community
- raise concerns or complaints directly with the school through the appropriate school procedures rather than attempting to resolve them through social media or online groups
- not use online platforms to bully, harass, threaten, discriminate against or make inappropriate comments about pupils, staff or other members of the school community
- not discuss or attempt to resolve incidents involving other pupils through social media, messaging groups or other public or private online forums
- respect the privacy and confidentiality of pupils, families and staff
- not share photographs, videos or other identifiable information about children other than their own without appropriate permission.

Where online activity raises a safeguarding concern, the school will respond in accordance with its **Safeguarding and Child Protection Policy**. Other inappropriate online conduct may be addressed through the school's complaints procedures or other relevant policies as appropriate.

Parents and carers will be asked to acknowledge the school's acceptable-use expectations.

7.3 Communicating with parents/carers about pupil activity

The school will provide parents and carers with appropriate information about the online platforms, digital services and technology pupils are expected to use as part of their learning.

Where pupils are asked to use a particular website, application, online service or digital platform, parents/carers will be given relevant information where appropriate, including the purpose of its use and any important online safety expectations.

Where an activity involves communication or interaction with people outside the school, parents/carers will be informed where appropriate about the nature and purpose of that interaction.

Parents and carers will be given information and guidance to support safe and responsible use of technology at home, including where online activity forms part of homework or home learning.

Parents and carers are encouraged to contact the school if they have any questions or concerns about an online platform, digital activity or aspect of their child's online safety.

8. Data security

The school is responsible for maintaining appropriate technical and organisational measures to protect its ICT systems, devices, accounts and data from unauthorised access, loss, damage, disclosure and cyber security threats.

The school will take proportionate steps to protect the confidentiality, integrity and availability of its systems and information and will maintain appropriate arrangements for preventing, identifying and responding to cyber security incidents.

All users of school ICT facilities and systems have a responsibility to follow safe and secure working practices and must report suspected cyber security incidents, data breaches, compromised accounts, phishing attempts, malware or other security concerns promptly.

The school will have regard to the Department for Education's current **Digital and Technology Standards**, including the cyber security standards for schools and colleges, and will periodically review its arrangements to ensure that appropriate safeguards remain in place.

Cyber security will form part of the school's wider oversight of safeguarding, data protection and technology. Appropriate information about the school's cyber security arrangements and compliance with relevant DfE standards will be provided to governors to support effective scrutiny and oversight.

8.1 Passwords

All users must take appropriate steps to keep their school accounts and login credentials secure.

Users must:

- use strong passwords in accordance with the school's ICT security requirements
- keep passwords, PINs and authentication details confidential and not share them with others
- use only their own account and must not knowingly access another person's account
- use multi-factor authentication (MFA) where this is required or made available by the school
- not approve unexpected MFA requests or provide authentication codes to another person
- log out or securely lock devices when leaving them unattended
- report suspected compromised accounts, passwords or unauthorised access promptly to the appropriate member of staff or ICT support.

Staff must not allow pupils to use staff accounts or access systems using staff login credentials.

Pupils will be taught age-appropriate approaches to password and account security and must not share their individual school login details with other pupils.

Access permissions will be appropriate to the user's role and will be reviewed or removed when no longer required.

Deliberately sharing account credentials, accessing another person's account without authorisation or attempting to gain unauthorised access to school systems may result in action under the school's relevant behaviour or disciplinary procedures.

8.2 Software updates, firewalls and anti-virus software

The school will maintain appropriate security measures to protect its devices, networks, systems and data from cyber security threats.

School-managed devices and systems will, where appropriate:

- use supported and appropriately licensed software and operating systems
- have security updates and patches installed within appropriate timescales, with automatic updates enabled where suitable
- use appropriate firewall, anti-malware and other security protections
- be securely configured to reduce the risk of unauthorised access
- have unnecessary accounts, software and services removed or disabled where appropriate.

Users must not disable, remove, alter or attempt to circumvent security controls, software updates, firewalls, anti-malware protection, filtering, monitoring or other technical safeguards without specific authorisation.

Staff must not install unauthorised software, applications, browser extensions or other services on school-managed devices or systems.

Any warning, suspected malware, unusual device behaviour or other potential cyber security concern must be reported promptly to the appropriate ICT support.

The school will work with its ICT support provider to ensure that security arrangements are regularly reviewed and updated in response to identified vulnerabilities, changes to technology and emerging cyber security risks.

8.3 Data protection

All personal data must be collected, processed, stored, shared and disposed of in accordance with applicable data protection legislation and the school's **Data Protection Policy**.

Users must:

- only access personal or confidential information where this is necessary for their role
- only use school-approved systems and services to store, process or share school information
- take appropriate care when sending, sharing or displaying personal or confidential information
- not upload personal, confidential, safeguarding or sensitive information to unauthorised websites, applications, cloud services or artificial intelligence tools
- ensure that personal data is not left visible or accessible to unauthorised individuals
- report any actual or suspected loss, unauthorised disclosure, accidental sharing or other personal data breach immediately in accordance with the school's Data Protection Policy and data breach procedures.

The use of artificial intelligence tools to process school information or personal data must comply with the school's **Artificial Intelligence (AI) Use Policy**.

Where there is uncertainty about whether information can be accessed, stored, shared or processed in a particular way, staff should seek advice before doing so.

8.4 Access to facilities and materials

Access to school systems, files, devices and information will be granted according to the user's role and responsibilities.

Users must not access, or attempt to access, systems, files, accounts or information for which they have not been authorised.

If a user is accidentally provided with access to information or systems that they believe they should not be able to access, they must **not view, copy, share or alter the information** and must report the issue promptly to an appropriate senior member of staff or ICT support.

Users must take reasonable steps to prevent unauthorised access to school systems and information, including locking devices when left unattended and logging out of systems when appropriate.

Access permissions will be reviewed and amended or removed when they are no longer required.

8.5 Encryption

The school will ensure that school-managed devices, systems and data are protected by appropriate security and encryption measures where required.

Personal, confidential or sensitive school information must only be stored or transferred using **school-approved devices, systems and services**.

Removable storage devices, including USB drives, must only be used for school information where they have been authorised and appropriate security measures are in place. Staff must not use unknown or unauthorised removable media on school devices.

Staff must not routinely download or store school personal data on personal devices, personal cloud-storage accounts or other unauthorised systems.

Where there is an authorised need to access school information remotely, staff must use the school's approved secure arrangements, including the school's **VPN where appropriate**, and comply with the requirements set out in section 5.3.

Lost or stolen devices or removable media containing, or potentially providing access to, school information must be reported **immediately** in accordance with the school's data breach and cyber security procedures.

9. Protection from cyber attacks

The school recognises that cyber security is essential to protecting its pupils, staff, systems, information and the continuity of school operations.

The school will work with its ICT support provider and Governing Body to maintain appropriate protection against cyber attacks and to have effective arrangements for identifying, reporting and responding to cyber security incidents.

The school will:

- have regard to the Department for Education's current **Cyber Security Standards for Schools and Colleges** and regularly review its arrangements against these standards
- maintain appropriate firewall, filtering, monitoring, anti-malware and other technical security measures
- keep operating systems, software, applications and devices appropriately updated and supported
- manage user accounts and access permissions appropriately, including removing or changing access when it is no longer required
- use multi-factor authentication where required or appropriate
- maintain appropriate backup arrangements for important school data and systems and ensure that recovery arrangements are appropriately tested
- provide staff with appropriate cyber security awareness and training, including recognising phishing, suspicious links, malicious attachments and attempts to obtain login information
- maintain appropriate procedures for responding to cyber security incidents and data breaches
- ensure suspected cyber attacks, compromised accounts, malware, phishing or other security incidents are reported promptly to ICT support and senior leaders
- consider cyber security when introducing new devices, systems, software and online services
- provide governors with appropriate information and evidence to enable them to scrutinise the school's cyber security arrangements.

The school will review its cyber security arrangements following significant cyber security incidents affecting the school or where incidents affecting **other organisations, systems or service providers indicate a potential risk to the school**.

Users must not attempt to disable, circumvent or interfere with the school's cyber security measures. They must report suspected security weaknesses or incidents promptly rather than attempting to investigate or resolve significant cyber security incidents themselves.

Where a cyber security incident may also constitute a safeguarding concern or personal data breach, the school's safeguarding and/or data breach procedures will also be followed.

The school will maintain an appropriate **cyber incident response plan**, developed with ICT support, setting out how significant cyber incidents will be managed, including responsibilities, communication arrangements, escalation and external reporting where required. The plan will be reviewed and tested periodically and following a significant cyber security incident or identified change in risk.

10. Internet access

The school provides secure internet access to support teaching, learning and the effective operation of the school.

Access to the school network and internet is subject to appropriate security, filtering and monitoring arrangements as set out in **section 5.5 of this policy**.

Access arrangements and permissions may differ according to the type of user, device and educational or professional need. Appropriate controls will be applied to pupil, staff and other authorised access.

Users must not attempt to bypass, disable or circumvent the school's network security, filtering or monitoring arrangements.

Any concern that inappropriate or harmful content can be accessed, that legitimate educational content is being unreasonably blocked, or that filtering or monitoring is not operating effectively must be reported promptly in accordance with section 5.5.

Internet access may be restricted or withdrawn where necessary to protect safeguarding, security or the effective operation of the school.

10.1 Pupils

Pupils will access the internet using **school-managed devices and authorised school network connections** under the direction and supervision of staff.

Pupils must not connect personal devices to the school network or Wi-Fi unless specifically authorised by the school for an agreed purpose.

Pupil internet access will be subject to the school's filtering and monitoring arrangements. Pupils must use their own individual account or allocated device where provided and must not use another pupil's login or allocated device without permission.

Pupils must not attempt to bypass filtering, monitoring or other security controls, including through the use of VPNs, proxy services, alternative networks or other methods.

Pupils will be taught how to use the internet safely, responsibly and critically through the school's curriculum and wider online safety provision and will be encouraged to report anything online that worries, upsets or concerns them to a trusted adult.

Where access to generative AI or other emerging technologies is permitted, this will be teacher-directed, age-appropriate and in accordance with the school's **Artificial Intelligence (AI) Use Policy**.

10.2 Parents/carers and visitors

Parents/carers, visitors, contractors and other external users will not normally be permitted to access the school's network or Wi-Fi unless access is required for an authorised purpose.

Where access is provided, users must:

- use only the network, account or access arrangements provided or authorised by the school
- comply with the school's acceptable-use, safeguarding and security expectations
- not attempt to access school systems, files or information for which they have not been authorised
- not attempt to bypass or interfere with the school's filtering, monitoring or security arrangements
- report any security, safeguarding or inappropriate-content concerns promptly to a member of staff.

Staff must not provide network passwords, login credentials or other access information to unauthorised individuals.

The school may restrict or withdraw network access at any time where this is necessary for safeguarding, security or operational reasons.

Where appropriate, visitors or other external users who require access to school ICT systems or networks will be made aware of, and expected to comply with, the school's acceptable-use requirements.

11. Monitoring and review

The Headteacher, DSL and appropriate senior leaders will monitor the implementation and effectiveness of this policy, supported by the school's ICT support provider where appropriate.

The school will review this policy **at least annually**, and sooner where required following:

- changes to legislation, statutory guidance or Department for Education standards
- significant changes to the school's technology, systems or online services
- a significant online-safety, safeguarding, data-protection or cyber-security incident
- concerns about the effectiveness of filtering or monitoring arrangements
- the identification of new or emerging online risks or technologies.

The review of this policy will form part of the school's wider review of **online safety provision**, including consideration of filtering and monitoring, cyber security, emerging technologies and artificial intelligence.

The school will maintain appropriate evidence of reviews, checks and resulting actions. Identified actions will be allocated appropriately and monitored to completion.

The Governing Body will receive appropriate information to enable it to provide oversight and challenge in relation to online safety, filtering and monitoring and cyber security.

The Governing Body is responsible for approving this policy. The policy will record its approval date, review date and the person responsible for its implementation.

12. Related policies

This policy should be read alongside the school's other relevant policies and procedures, including:

- Safeguarding and Child Protection Policy

- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy and data breach procedures
- Mobile Phone and Smart Devices Policy
- Artificial Intelligence (AI) Use Policy
- Photography and Image-Sharing Policy
- Acceptable Use Agreements for pupils, parents/carers, staff, governors, volunteers and visitors
- relevant cyber-security and ICT procedures.

These documents collectively support the school's approach to safeguarding children and adults when using technology and ensure that online safety is embedded within the school's wider safeguarding arrangements.

Senior Leadership Team: September 2026

To be reviewed: June 2027

Appendix 1 – Acceptable Use Agreement for Parents and Carers

The school uses technology to support learning and to communicate with families. We also teach children how to use technology safely and responsibly.

I will...	I will not...
Be respectful when communicating with school staff, other parents and children.	Use social media, messaging groups or other online spaces to complain about or criticise individual staff, pupils or families.
Raise concerns or complaints directly with the school so they can be dealt with properly.	Try to sort out problems involving other children through social media or group chats.
Respect the privacy of children, families and staff.	Share photos, videos or personal information about other children without permission.
Support my child to use technology safely and responsibly.	Encourage my child to get around school filtering, monitoring or online-safety rules.
Encourage my child to tell a trusted adult if something online worries or upsets them.	Ask my child to use AI or other online tools in a way that goes against school rules.

I understand that:

✓	The school uses filtering and monitoring systems to help keep children safe online.
✓	Children are expected to follow the school's pupil Acceptable Use Agreement.
✓	The school may look into online behaviour outside school if it affects a child's safety, wellbeing or learning in school.
✓	Use of artificial intelligence (AI) in school is controlled by staff and must follow the school's AI Policy.
✓	I can contact the school if I am worried about my child's online safety.

Parents and carers are asked to confirm each year that they have read and agree to these expectations.

Appendix 2 – Acceptable Use Agreement for KS2 Pupils

My rules for using technology safely

We use computers, iPads and the internet to help us learn. These rules help to keep **me and other people safe**.

I will...	I will not...
Use computers and iPads for my learning and follow the instructions my teacher gives me.	Search for, look at or share things that I know are not suitable for children.
Use my own login and the iPad or device I have been given.	Use someone else's login, password or device without permission.
Keep my password to myself.	Share my password or try to find out someone else's.
Be kind and respectful to other people online.	Send or post anything that is unkind, rude or could upset someone.
Stop and ask an adult if I am unsure about a website, link, message or download.	Click strange links, download things or install apps without permission.
Tell a trusted adult straight away if I see something that worries, scares or upsets me.	Try to get around the school's internet safety or monitoring systems.
Keep personal information about myself and other people private.	Share private information, photos or videos of myself or other people without permission.
Only use AI when my teacher says I can and use it in the way they have shown me.	Use AI to do my work for me or pretend that AI's work is my own.
Tell an adult if I make a mistake or something goes wrong.	Hide a problem because I am worried I might get into trouble.

I understand that:

- ✓ The school checks and monitors how its computers, iPads and internet are being used to help keep everyone safe.
- ✓ What I do using my school login or school device can be linked to me.
- ✓ The school's online-safety rules are there to protect me and other people.
- ✓ If something happens online outside school that affects someone at school, I should tell a trusted adult.
- ✓ If I choose not to follow these rules, the school may limit my use of technology and take further action.

My agreement

By clicking “I agree”, I am saying that I understand these rules and will try my best to follow them.

Appendix 3 – Acceptable Use Agreement for Younger Pupils

🌟 My Technology Rules 🌟

These rules help to keep me safe.

	I will...
	Ask an adult before I use technology.
	Be kind when I am online.
	Keep my password private.
	STOP if I see something that worries or scares me.
	TELL an adult straight away.
	ASK if I am not sure what to do.
	Keep information about me private.
	Tell the truth if I make a mistake.

★ Remember ★

 Adults at school help to keep me safe online.

 School computers and iPads are checked to help keep me safe.

 **STOP and TELL** if something doesn't feel right.

 I use technology **safely and kindly**.

My agreement

I understand my technology rules. I will try my best to follow them. 🌟

Appendix 4 – Acceptable Use Agreement for Adults

Using school technology safely and responsibly

This agreement applies to adults who are given access to the school's devices, systems, accounts, network or online services.

The school's technology should be used safely, responsibly and professionally. Safeguarding, confidentiality, data protection and cyber security must be considered at all times.

When using school technology, systems and online services, I agree to:

I agree to:
Keep my passwords and login details secure and use only my own account.
Use school devices, systems and accounts responsibly and only for authorised purposes.
Maintain appropriate supervision when pupils are using technology and remain alert to online-safety concerns.
Follow the school's filtering and monitoring arrangements and report concerns or weaknesses promptly.
Report online safeguarding concerns promptly to the DSL/DDSL and follow the school's safeguarding procedures.
Keep personal, confidential and safeguarding information secure and use approved school systems to store, access or share it.
Be alert to phishing, suspicious emails, links and attachments and report anything suspicious.
Use AI only in accordance with the school's Artificial Intelligence (AI) Use Policy and never enter safeguarding, confidential or sensitive personal information into unauthorised AI tools.
Follow school expectations when using personal phones, devices, social media and online communication.
Not share passwords or authentication codes or allow another person to use my account.
Not access, create, store or share illegal, harmful or inappropriate material.
Not attempt to bypass or interfere with filtering, monitoring or security systems unless specifically authorised to carry out an approved test.
Not access, change or share information that I am not authorised to access.
Not install unauthorised software, apps or devices on school systems.
Not store school, pupil or safeguarding information on personal accounts, devices or cloud storage unless specifically authorised.
Report lost or stolen devices, compromised accounts, data breaches and other cyber-security concerns promptly.

Monitoring

I understand that the school uses appropriate **filtering and monitoring systems** to support safeguarding, security and responsible use of technology.

I understand that my use of school systems, accounts, devices and internet access may be monitored and reviewed in accordance with school policy.

My agreement

By clicking "I agree", I confirm that I have read and understood these expectations and agree to follow the school's Acceptable Use Policy and other relevant school policies