



St Joseph's Catholic Voluntary Academy



With God's Guidance We Love, Learn, Respect and Forgive

Part of the St Thomas Aquinas Catholic Multi-Academy Trust

DIGITAL TECHNOLOGY AND ACCEPTABLE USE POLICY

Implementation	Whole school community
School monitoring lead	Mrs Clair Dedman
Approved by	Local Governing Body / Headteacher
Policy status	School-level policy within St Thomas Aquinas Catholic Multi- Academy Trust arrangements
Effective from	24 August 2026
Signed (Head Teacher)	
Signed (Chair of Governors)	
Review cycle	At least every two years, and earlier where guidance, technology or Trust arrangements change
Next formal review	January 2028

Contents

1. Introduction and aims
2. Scope and relationship with Trust arrangements
3. Legislation, statutory guidance and standards
4. Definitions
5. Roles and responsibilities
6. Acceptable and unacceptable use
7. Staff, governors, volunteers, contractors and visitors
8. Pupils
9. Parents and carers
10. Artificial intelligence (AI)
11. Online safety and the 4Cs
12. Filtering and monitoring
13. Cyber security, information security and access management
14. Data protection and confidentiality
15. Internet, network, cloud and remote access
16. Email, messaging and digital communication
17. Personal devices, mobile phones and removable media
18. Social media and online professional conduct
19. Images, video, audio and digital content
20. Digital wellbeing and curriculum
21. Responding to incidents and concerns
22. Monitoring, training and review
23. Related policies and guidance
- Appendix 1: Staff social media and online professional conduct guidance
- Appendix 2: Parent/carers acceptable use agreement
- Appendix 3: Older pupil acceptable use agreement
- Appendix 4: Younger pupil acceptable use agreement
- Appendix 5: Staff/governor/volunteer/visitor acceptable use agreement

1. Introduction and aims

Digital technology is an integral part of life at St Joseph's Catholic Voluntary Academy. It supports teaching and learning, communication, safeguarding, administration, inclusion and access to information. Used well, digital technology can enhance learning, creativity, collaboration and participation. It can also create risks relating to safeguarding, online safety, data protection, cyber security, inappropriate content and misuse.

This policy sets out clear expectations for the safe, responsible, lawful and effective use of digital technology, school systems, devices, networks and online services. It reflects the school's Catholic ethos and our commitment to treating others with dignity, respect and care, both online and offline.

The aims of this policy are to:

- set clear expectations for all users of school digital technology, systems and services;
- protect pupils, staff and the wider school community from online and technology-related harm;
- support the school's safeguarding, child protection, data protection and cyber security arrangements;
- support pupils to become safe, responsible, discerning and respectful digital citizens;
- prevent disruption, loss, unauthorised access or misuse of school systems and data;
- promote appropriate, transparent and ethical use of emerging technologies, including generative artificial intelligence (AI);
- clarify the relationship between school-level responsibilities and the centrally managed technology arrangements provided by St Thomas Aquinas Catholic Multi-Academy Trust.

Breaches of this policy may be addressed under the school's Behaviour Policy, Staff Code of Conduct, Safeguarding and Child Protection Policy or other relevant procedures.

2. Scope and relationship with Trust arrangements

This is a school-level policy for St Joseph's Catholic Voluntary Academy. The school is part of St Thomas Aquinas Catholic Multi-Academy Trust (the Trust). The Trust is the proprietor of the academy and provides or oversees a number of central services and systems, including significant elements of IT infrastructure, technical support, cyber security, filtering and monitoring.

The school does not independently procure or technically manage Trust-wide filtering, monitoring, network security or other centrally managed infrastructure. These technical functions are undertaken through the Trust's IT arrangements. The school is responsible for implementing those arrangements locally, ensuring safe day-to-day use, supervising pupils, responding to safeguarding concerns, educating pupils about online safety and escalating technical concerns through the appropriate Trust channels.

Where this policy refers to 'Trust IT', this means the central or Trust-authorised IT team or service responsible for the relevant technical provision.

Where a Trust policy, standard or technical instruction applies, users must follow it in addition to this policy. If there is any conflict, the Trust requirement or statutory guidance takes precedence.

3. Legislation, statutory guidance and standards

This policy has regard to relevant legislation, statutory guidance and national standards, including:

- Keeping Children Safe in Education 2026 (in force from 1 September 2026);
- Working Together to Safeguard Children;
- Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Human Rights Act 1998;
- Equality Act 2010 and the Public Sector Equality Duty;
- Freedom of Information Act 2000;
- Education Act 2011 and current DfE guidance on searching, screening and confiscation;
- Education and Inspections Act 2006;
- Online Safety Act 2023, where relevant;
- Prevent Duty guidance;
- DfE Filtering and Monitoring Standards for schools and colleges;
- DfE Cyber Security Standards for schools and colleges;
- DfE Generative AI in Education guidance and Generative AI Product Safety Standards;
- DfE guidance on mobile phones in schools.

This policy should be read alongside the Trust and school policies listed in section 23.

4. Definitions

Digital technology: all devices, systems, networks, software, applications, websites, cloud services and digital communication tools used by or on behalf of the school, including technologies that may become available in future.

School systems and devices: technology supplied, licensed, managed or approved by the school or Trust, including desktops, laptops, tablets, interactive displays, phones, cameras, network services, cloud platforms and accounts.

Users: anyone authorised to use school or Trust digital technology, including pupils, staff, governors, volunteers, contractors and visitors.

Personal use: use that is not directly connected with the user's employment, education or authorised school purpose.

Authorised personnel: school leaders, Trust IT staff or other persons authorised to administer, support, monitor or manage digital systems.

Personal data: information relating to an identified or identifiable individual, as defined by data protection law.

Sensitive/confidential information: information requiring additional protection, including safeguarding information, special category personal data, pupil records, staff records and information not intended for public disclosure.

Generative AI: technology capable of generating or transforming content such as text, images, audio, video, code or other outputs in response to prompts or other inputs.

5. Roles and responsibilities

5.1 St Thomas Aquinas Catholic Multi-Academy Trust and Trust IT

The Trust is the proprietor of the academy. Trust-level arrangements include centrally managed or authorised technical services. In relation to this policy, Trust IT is responsible, as applicable, for the technical provision, configuration, maintenance and support of Trust-managed infrastructure and services, including filtering and monitoring technology, network security, technical access controls, software deployment, updates, backups and cyber security measures.

The school will use Trust-approved systems and follow Trust technical instructions and escalation routes.

5.2 Headteacher and senior leadership

The Headteacher has responsibility for the implementation of this policy at school level and for ensuring that staff understand their responsibilities.

In line with KCSIE 2026, an appropriate member of the senior leadership team will hold school-level responsibility for filtering and monitoring oversight. This does not make the school responsible for procuring or technically administering Trust filtering and monitoring systems. The role is to provide leadership oversight, participate in the required review with the DSL and Trust IT support, ensure issues are escalated and ensure the school can evidence that the review has taken place.

5.3 Designated Safeguarding Lead (DSL)

The DSL and deputies have a key role in online safety. The DSL will understand the filtering and monitoring systems and processes used in the school, support the annual effectiveness review, respond to safeguarding concerns identified through digital activity and ensure appropriate action is taken in accordance with the Safeguarding and Child Protection Policy.

The DSL will ensure that online safety is treated as an interrelated safeguarding theme and that staff know how to report concerns.

5.4 Local Governing Body

The Local Governing Body provides school-level oversight within the Trust's governance framework. Governors should be assured that the school is implementing Trust arrangements appropriately, that required reviews and safeguarding processes are taking place, and that leaders understand and fulfil their responsibilities. Technical procurement and management of centrally provided systems remains with the Trust.

5.5 All staff

- follow this policy, the Staff Code of Conduct and safeguarding procedures;
- use school and Trust systems responsibly and professionally;
- understand the school's filtering and monitoring expectations, including how to report and escalate concerns;
- supervise pupils' use of technology appropriately;
- report safeguarding, data protection, cyber security and technical concerns promptly;
- model safe, respectful, lawful and transparent use of technology, including AI.

6. Acceptable and unacceptable use

Users must use digital technology in a lawful, safe, respectful and responsible manner. The following are examples of unacceptable use:

- using technology to bully, harass, threaten, intimidate, discriminate against or deliberately upset another person;
- accessing, creating, requesting, storing, linking to, transmitting or sharing illegal, pornographic, extremist, hateful, abusive, violent or otherwise inappropriate content;
- making, requesting, altering, sending or sharing nudes or semi-nudes, including digitally altered or wholly AI-generated images, except where authorised safeguarding professionals are acting strictly in accordance with statutory guidance;
- attempting to access restricted systems, accounts, files or data without authorisation;
- sharing passwords, authentication codes or account credentials, or using another person's account;
- bypassing or attempting to bypass filtering, monitoring, security, device-management or access-control systems;
- using VPNs, proxy services or other mechanisms to evade school or Trust controls unless specifically authorised for a legitimate technical purpose;
- installing software, browser extensions, applications or services without appropriate authorisation;
- creating or using malware, scripts, tools or code intended to interfere with systems, accounts or data;
- causing deliberate damage to devices, systems, networks or data;
- accessing, changing, deleting, copying or disclosing information without permission;

- causing or contributing to a personal-data breach;
- using school systems to infringe copyright or intellectual property rights;
- impersonating another person or misrepresenting identity;
- using technology to bring the school, Trust or members of the school community into disrepute;
- using inappropriate or offensive language;
- using school technology for unauthorised commercial, political campaigning or private-business purposes;
- using generative AI in a way that breaches section 10 of this policy;
- failing to report known safeguarding, security or data-protection concerns.

This list is not exhaustive. The Headteacher, DSL and/or Trust will use professional judgement and applicable policies when considering behaviour not specifically listed.

6.1 Exceptions

There may be occasions when authorised staff need to access material or perform an action that would otherwise be restricted, for example for safeguarding, curriculum, investigation, testing or technical administration. Such activity must be necessary, proportionate, authorised and carried out in accordance with Trust and school procedures.

6.2 Sanctions

Misuse may result in restriction or removal of access, action under the Behaviour Policy or staff disciplinary procedures, safeguarding action, referral to the Trust, reporting to external agencies or law enforcement, or other proportionate action.

7. Staff, governors, volunteers, contractors and visitors

7.1 Accounts and access

- Users must use their own authorised account and must not allow others to use it.
- Passwords and multi-factor authentication information must be kept secure.
- Access rights are provided according to role and need. Users must not access information simply because technical access is possible.
- Unexpected or inappropriate access must be reported promptly to the appropriate school leader and/or Trust IT.
- Devices must be locked when unattended and users must log out when appropriate.

7.2 Professional and personal use

School and Trust technology is primarily provided for professional and educational purposes. Limited personal use may be permitted where this does not interfere with duties, take place during teaching time, involve pupils, create additional cost or risk, breach any policy, or constitute unacceptable use.

Users should have no expectation that personal activity conducted on school or Trust systems is private. Monitoring may take place in accordance with law, safeguarding requirements and Trust arrangements.

Personal files such as private photographs, music or videos should not be stored on school systems unless required for an authorised school purpose.

7.3 Confidentiality

Staff must take particular care with safeguarding information, pupil information, staff information and other confidential material. Information must only be accessed, shared or stored where there is a legitimate professional reason and through approved systems.

8. Pupils

8.1 Access and supervision

Pupils may use school devices, accounts, networks and online services for educational purposes under appropriate staff supervision and in accordance with age-appropriate acceptable use agreements.

Pupils must use only accounts and services made available or approved by the school or Trust. They must follow staff instructions and must not attempt to alter device settings, install software or circumvent controls.

8.2 Reporting concerns

Pupils will be taught to stop, close or move away from content that worries or upsets them where safe to do so, and to tell a trusted adult immediately. Pupils will not be blamed for accidentally encountering inappropriate content when they report it promptly.

8.3 Searching and confiscation

Where there are reasonable grounds and the legal requirements are met, the school may search, examine, confiscate or delete data from pupil devices in accordance with the Education Act 2011, current DfE guidance on searching, screening and confiscation, the Behaviour Policy and safeguarding procedures.

8.4 Online behaviour outside school

The school may respond to online behaviour occurring outside school where it affects safeguarding, the welfare of pupils or staff, the orderly running of the school, or falls within the scope of the Behaviour Policy or other applicable procedures. This may include online bullying, harassment, sharing harmful or explicit content, impersonation, threats, discrimination or misuse of school accounts.

9. Parents and carers

Parents and carers are important partners in helping children use technology safely and responsibly. The school will communicate relevant online-safety information and may provide information about the filtering and monitoring arrangements used on school systems.

Parents and carers are expected to:

- communicate respectfully with staff, pupils and other families;
- use official school channels for concerns or complaints;
- support age-appropriate and safe technology use at home;
- respect privacy and not share images, video or personal information about other children without appropriate permission;
- support the school's acceptable use expectations and discuss them with their child;
- report safeguarding or online-safety concerns to the school promptly.

10. Artificial intelligence (AI)

Generative AI can support teaching, learning, accessibility, creativity and administration, but it can also produce inaccurate, biased, inappropriate or harmful material and may create risks relating to safeguarding, privacy, intellectual property and academic integrity. AI must therefore be used with professional judgement and human oversight.

10.1 Approved and appropriate use

- Staff should use Trust- or school-approved AI tools and accounts where these are specified.
- Pupil-facing AI use must be purposeful, age-appropriate, supervised as appropriate and authorised by staff.
- Age restrictions and provider terms must be followed.
- AI should support, not replace, teaching, professional judgement, independent thinking or meaningful pupil learning.
- AI must not be relied upon as the sole basis for safeguarding, disciplinary, assessment, employment or other significant decisions about individuals.

10.2 Personal and confidential information

Users must not enter personal, special-category, safeguarding, confidential or otherwise sensitive information into a generative AI system unless the system and use have been specifically approved for that purpose and all relevant Trust/data-protection requirements have been met. This includes identifiable pupil work, reports, names, photographs, case information and staff information.

10.3 Accuracy, bias and verification

AI outputs may be inaccurate, incomplete, fabricated or biased. Staff remain responsible for checking factual accuracy, suitability, age appropriateness, tone, bias and copyright implications before using AI-generated material professionally or with pupils.

10.4 Transparency and accountability

- Staff and pupils should be open about significant use of AI where it has contributed to work, decisions or published content.
- AI-generated material must not be presented misleadingly as entirely human-created where acknowledgement is appropriate.
- Pupils must not submit AI-generated work as their own where this would misrepresent their knowledge, understanding or authorship.
- Teachers may ask pupils to explain their thinking, sources, drafting process or use of AI.
- Staff must model ethical and transparent use and remain accountable for material they choose to use.

10.5 Safeguarding and harmful AI content

AI may generate or facilitate harmful content or simulated human interaction. Concerns involving AI chatbots, companion-style systems, harmful prompts, manipulated media, deepfakes, deep nudes, grooming-like interactions, sexualised content or other safeguarding risks must be reported to the DSL in the same way as other online-safety concerns.

10.6 Intellectual property

Users must respect copyright and intellectual property when using AI. Staff should not upload copyrighted, confidential or pupil-created material to AI services for model training, commercial reuse or other purposes unless this is authorised and lawful.

11. Online safety and the 4Cs

Online safety is a running and interrelated theme within safeguarding, curriculum, staff training, parental engagement and the work of the DSL. The school uses the 4Cs framework to understand online risk:

Content: exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, antisemitism, self-harm, suicide, extremism, radicalisation, extreme violence, misinformation, disinformation and conspiracy theories.

Contact: harmful interaction with other users or generative AI applications that simulate human interaction, including peer pressure, grooming, exploitation, adults posing as children, harmful chatbot or companion interactions and inappropriate commercial contact.

Conduct: online behaviour that causes or increases the likelihood of harm, including bullying, harassment, making, sending or receiving explicit images, including AI-generated images, impersonation and harmful sharing.

Commerce: risks such as gambling, inappropriate advertising, phishing, scams, financial exploitation and other harmful commercial practices.

The school recognises that some pupils, including pupils with SEND or other vulnerabilities, may experience additional or different online risks and may require adapted teaching, supervision or support.

12. Filtering and monitoring

Appropriate filtering and monitoring are essential safeguarding measures. At St Joseph's, the technical filtering and monitoring systems are provided, configured, maintained and supported through St Thomas Aquinas Catholic Multi-Academy Trust IT arrangements. The school does not independently source or technically administer these systems.

12.1 School-level oversight

In accordance with KCSIE 2026, the effectiveness of filtering and monitoring arrangements will be reviewed at least once every academic year. The review will be led by the identified SLT member responsible for filtering and monitoring, with the support of the DSL and Trust IT support.

The review will include appropriate checks that filtering is working on internet-connected devices in relevant school locations. Records of checks and the review will be retained. Where the technical checking is undertaken by Trust IT, the school will ensure that suitable evidence or confirmation is available for school-level safeguarding oversight.

The school will ensure that:

- leaders and relevant staff understand the filtering and monitoring provision in place;
- staff know how to report or escalate concerns;
- technical concerns or requests for changes are referred to Trust IT through the appropriate process;
- safeguarding concerns arising from monitoring are referred to the DSL;
- filtering does not knowingly and unreasonably interfere with legitimate teaching and learning;
- the needs, ages and vulnerabilities of pupils are considered in school-level review and safeguarding discussions;
- AI-related risks are considered as part of filtering and monitoring arrangements.

12.2 Staff expectations

Filtering is not a substitute for supervision, education or professional vigilance. Staff must supervise pupils appropriately and report inappropriate content, suspected filtering failures, unusual access or safeguarding concerns promptly. Staff must not attempt to disable or circumvent filtering or monitoring.

13. Cyber security, information security and access management

Cyber security is a safeguarding issue as well as a technical issue. Compromised accounts, unavailable systems, stolen data or altered safeguarding records can create direct risks to children.

Technical cyber security controls are primarily managed through Trust IT arrangements. All users must support these controls by following safe practice.

13.1 Passwords and authentication

- Use strong, unique passwords or passphrases in accordance with Trust requirements.
- Do not disclose passwords, authentication codes or recovery information.
- Use multi-factor authentication where provided or required.
- Do not approve unexpected authentication requests.
- Report suspected account compromise immediately.

13.2 Phishing, malware and suspicious activity

- Treat unexpected links, attachments, QR codes, login prompts and requests for money or information with caution.
- Do not install unauthorised software or disable security tools.
- Report suspected phishing, malware, ransomware, account compromise or other cyber incidents promptly to Trust IT and school leaders as appropriate.
- Disconnect or stop using a device if instructed by Trust IT following a suspected incident.

13.3 Updates, backups and security controls

Trust-managed devices and systems will be subject to centrally managed updates, security controls and backup arrangements where applicable. Users must not interfere with these measures and must allow required updates or restarts to take place.

13.4 Access management

Access will be based on role and legitimate need. Staff must notify the appropriate person when access appears excessive, missing or incorrect. Accounts must not be shared. Access for leavers or role changes will be managed through school and Trust procedures.

14. Data protection and confidentiality

St Thomas Aquinas Catholic Multi-Academy Trust is the data controller for its academies. Personal data must be processed in accordance with Trust data-protection policies, privacy notices and applicable data-protection law.

- Only collect, access, use or share personal data for an authorised and legitimate purpose.
- Use approved school or Trust systems for storing and sharing school information.

- Apply appropriate access permissions and check recipients before sending information.
- Do not use personal email, personal cloud storage or unauthorised applications for school personal data.
- Take particular care with safeguarding information and special-category data.
- Report actual or suspected data breaches immediately through the school/Trust data-breach process.
- Do not retain information longer than required by applicable retention arrangements.

14.1 Encryption and removable media

School data must only be stored on removable media or personal devices where specifically authorised and where the device or media meets Trust security requirements, including encryption where required. Unauthorised USB drives or storage devices must not be used for school personal data.

15. Internet, network, cloud and remote access

15.1 Internet and Wi-Fi

School internet access is protected by Trust-managed security, filtering and monitoring arrangements. Pupils access the network using school-managed or authorised devices and accounts under appropriate supervision.

Parents, visitors and contractors may only access school or guest connectivity where authorised. Staff must not disclose Wi-Fi credentials to unauthorised persons.

15.2 Cloud services

Staff must use approved cloud services, including Trust-provided Microsoft services where applicable. Confidential information must not be transferred to unapproved consumer cloud services.

15.3 Remote access and working away from school

- Use approved remote-access and cloud services.
- Protect screens and conversations from being seen or overheard by unauthorised people.
- Do not leave devices or confidential papers unattended in insecure locations.
- Use secure networks and follow Trust instructions regarding public Wi-Fi.
- Report loss or theft of any device containing or capable of accessing school information immediately.

16. Email, messaging and digital communication

School-provided email and approved communication systems must be used for school business. Staff must not use personal email accounts or personal messaging accounts to communicate with pupils or to conduct confidential school business.

- Check recipients carefully, particularly when using reply-all, distribution lists or autofill.
- Use BCC where appropriate when emailing groups of external recipients.
- Take care with confidential or sensitive attachments and use approved secure methods.
- Do not open suspicious attachments or links.
- If an email or message is received in error, notify the sender where appropriate, do not use or disclose the information, and delete it securely.
- If information is sent to the wrong recipient, report it immediately as a potential data breach.
- Remember that school communications may be retrievable and disclosable under legal or information-rights processes.

17. Personal devices, mobile phones and removable media

Personal devices must be used in accordance with the school's Mobile Phone Policy, Staff Code of Conduct and safeguarding expectations. KCSIE 2026 states that schools should be mobile-phone-free environments for pupils by default; the school's separate Mobile Phone Policy sets out the detailed arrangements for pupils.

Staff must not use personal devices to photograph or record pupils unless specifically authorised under school procedures. Personal devices must not be used to store school personal data unless expressly authorised and compliant with Trust security requirements.

Pupil personal devices brought to school are subject to the school's Behaviour and Mobile Phone policies and may be searched or confiscated where lawful and appropriate.

18. Social media and online professional conduct

Staff, governors, volunteers and others acting on behalf of the school must maintain professional boundaries online. This applies across social networks, messaging applications, group chats, gaming platforms, forums, livestreaming services and emerging platforms.

- Do not accept or initiate personal social-media connections with current pupils.
- Do not communicate privately with pupils through personal accounts.
- Exercise great caution in relation to connections with parents/carers where this could blur professional boundaries.
- Do not post confidential information, pupil information or internal school matters.
- Do not post content that could reasonably undermine professional standing, safeguarding responsibilities or trust in the school.
- Use appropriate privacy and security settings, while recognising that online content can be copied, shared or made public.
- Do not use school logos, branding or identity to imply official school endorsement without authorisation.

- Report online harassment, impersonation, threats or safeguarding concerns through appropriate school procedures.

Further practical guidance is provided in Appendix 1.

19. Images, video, audio and digital content

Photographs, video and audio involving pupils must be created, stored, used and shared in accordance with safeguarding, consent, data-protection and school procedures.

- Use school-authorised devices and systems where required.
- Do not publish identifiable pupil content unless the relevant permissions and school procedures permit this.
- Do not alter images or media in a misleading, humiliating, sexualised or harmful way.
- AI-generated or digitally manipulated images of real members of the school community must not be created or shared in a way that is deceptive, abusive, sexualised, discriminatory or harmful.
- Any concern involving nudes or semi-nudes, including AI-generated or digitally altered imagery, must be reported immediately to the DSL and managed under safeguarding procedures.

20. Digital wellbeing and curriculum

The school teaches pupils how to use technology safely, respectfully and critically through the computing curriculum, relationships/health education, safeguarding education and other relevant curriculum opportunities.

Teaching will include, as age appropriate:

- privacy, passwords and protecting personal information;
- online relationships, respectful communication and cyberbullying;
- recognising misinformation, disinformation, scams and manipulation;
- digital footprint, reputation and permanence;
- healthy and balanced use of technology;
- copyright and ownership;
- reporting harmful or worrying content;
- the 4Cs of online risk;
- safe, ethical and transparent use of AI, including understanding that AI can be wrong, biased or manipulative;
- age-appropriate understanding of manipulated media, deepfakes and AI-generated content.

21. Responding to incidents and concerns

21.1 Safeguarding and online-safety concerns

Any concern that a child may be at risk of harm must be reported immediately in accordance with the Safeguarding and Child Protection Policy. Technology-related concerns are safeguarding concerns where they involve risk of harm.

21.2 Filtering or monitoring concerns

Suspected filtering failures, inappropriate access or monitoring issues must be reported to the identified school lead/DSL as appropriate and escalated to Trust IT for technical investigation. The school will not independently alter centrally managed controls.

21.3 Cyber incidents

Suspected cyber incidents must be reported promptly to Trust IT and relevant school leaders. Users should preserve evidence and follow technical instructions rather than attempting their own investigation or remediation.

21.4 Data breaches

Actual or suspected loss, unauthorised disclosure, alteration or access to personal data must be reported immediately through the school/Trust data-breach procedure.

21.5 Nudes and semi-nudes

Incidents involving the making or sharing of nudes and semi-nudes, including self-generated, digitally altered, deepfake, deep-nude or wholly AI-generated imagery involving a person under 18, will be managed as safeguarding matters in accordance with KCSIE and relevant UKCIS guidance. Staff must not copy, print, forward or unnecessarily view such imagery.

22. Monitoring, training and review

22.1 Monitoring

The school and Trust reserve the right to monitor use of school and Trust systems in accordance with law, safeguarding responsibilities and applicable Trust arrangements. This may include internet activity, account access, network logs, email or other electronic communications where lawful and proportionate.

Monitoring is undertaken for legitimate purposes such as safeguarding, system security, investigating policy compliance, preventing or detecting crime, responding to legal obligations and maintaining effective operation.

22.2 Training

Staff safeguarding training will include online safety and an understanding of filtering and monitoring expectations, relevant roles and responsibilities, and how to report and escalate concerns. Relevant staff will receive additional training appropriate to their roles.

Pupils receive regular age-appropriate online-safety education. Parents and carers will be supported with relevant information where appropriate.

22.3 Review

This policy will be reviewed at least every two years and sooner where there are significant changes to legislation, statutory guidance, Trust arrangements, technology or identified risks. Filtering and monitoring effectiveness will be reviewed at least once every academic year, separately from the general policy review cycle.

23. Related policies and guidance

This policy should be read alongside current versions of relevant school and Trust documents, including:

- Safeguarding and Child Protection Policy;
- Staff Code of Conduct;
- Behaviour Policy;
- Data Protection Policy and privacy notices;
- Mobile Phone Policy;
- Online Safety arrangements/guidance;
- Remote Education or Remote Learning guidance, where applicable;
- Complaints Policy;
- Freedom of Information and records-retention arrangements;
- Trust cyber security, IT support and technical-use requirements;
- any current Trust acceptable-use or information-security standards.

Appendix 1: Staff social media and online professional conduct guidance

This guidance replaces the former Facebook-specific appendix. It applies to all social media, messaging services, forums, gaming platforms, livestreaming services and other online spaces.

Protect your professional boundaries

- Keep personal and professional communication separate.
- Do not add, follow or privately message current pupils using personal accounts.
- Do not use personal accounts to discuss individual pupils, families, colleagues or confidential school matters.
- Think carefully before accepting or initiating social media connections with parents/carers. Existing personal relationships should not be used for school communication, and professional boundaries must be maintained at all times.
- Do not use personal accounts to conduct school business where an approved school channel is available.

Protect your privacy and security

- Review privacy and security settings regularly.
- Use strong passwords and multi-factor authentication where available.
- Be cautious about location sharing, tagging, public profiles and information that identifies your workplace or routine.
- Remember that screenshots and copies can make supposedly private content permanent or public.
- Search your own name periodically if useful to understand what information is publicly visible.

Think before you post

- Do not post anything about pupils or confidential school matters.
- Do not share photographs or recordings taken for school purposes through personal accounts.
- Do not post content that is discriminatory, threatening, abusive or incompatible with professional responsibilities.
- Be aware that likes, shares, comments and group memberships can also be visible and may affect professional reputation.

If a pupil contacts or follows you

- Do not engage in personal conversation.
- Decline, remove or block the contact as appropriate.
- Retain evidence if the contact is concerning or persistent.
- Inform the DSL or a senior leader where there is a safeguarding, boundary or conduct concern.

If you experience harassment or impersonation online

- Do not retaliate.

- Preserve evidence such as screenshots, dates, usernames and URLs where safe to do so.
- Use platform reporting/blocking tools.
- Inform a senior leader and follow safeguarding or staff-support procedures.
- Where threats, hate crime, stalking or other criminal behaviour may be involved, senior leaders will consider referral to the police or other appropriate agency.

Appendix 2: Acceptable use agreement for parents and carers

Name of parent/carers: _____

Name of child: _____

Digital communication is an important part of school life. I understand that I have a role in modelling safe and respectful online behaviour.

When communicating with or about the school, I will:

- be respectful towards staff, pupils and other parents/carers;
- use official school channels for concerns or complaints;
- support my child to follow the school's acceptable-use expectations;
- talk to my child about safe and responsible technology use;
- report safeguarding or online-safety concerns to the school;
- respect the privacy of other children and families.

I will not:

- use members of staff's personal social media accounts to contact them about school matters; I will use the school's official communication channels instead.
- use social media, messaging groups or other online spaces to harass, threaten or abuse members of the school community;
- attempt to resolve concerns about another child by publicly identifying or criticising that child or family online;
- share photographs, video or personal information about children other than my own without appropriate permission;
- encourage my child to bypass school filtering, security or acceptable-use rules.

Signed: _____ Date: _____

Appendix 3: Acceptable use agreement for older pupils

Name of pupil: _____

When I use school devices, accounts, the internet or other digital technology, I will:

- use technology for learning and other purposes my teacher has allowed;
- use my own account and keep my password private;
- be kind and respectful to other people online;
- look after school equipment;
- tell an adult straight away if I see something worrying, upsetting or inappropriate;
- be honest about my use of AI and follow my teacher's instructions;
- check information carefully and remember that websites and AI can be wrong;
- respect other people's privacy, work and copyright.

I will not:

- try to access inappropriate or blocked websites or content;
- use VPNs (Virtual Private Network), proxies or other methods to bypass school controls;
- change settings, install apps or software without permission;
- use another person's account or share my login details;
- bully, threaten, embarrass or deliberately upset someone online;
- take, alter or share photographs, video or audio of other people without permission;
- make, request, send or share nudes or semi-nudes, including AI-generated or altered images;
- use AI to pretend work is entirely my own when it is not;
- try to damage, hack or interfere with school devices, accounts, networks or data.

I understand that the school and Trust may monitor my use of school systems to help keep people safe and protect the network. I understand that the school may respond to serious online behaviour even when it happens outside school.

Pupil signature: _____ Date: _____

Parent/carers: I have discussed this agreement with my child and support the school's expectations.

Parent/carers signature: _____ Date: _____

Appendix 4: Acceptable use agreement for younger pupils

Name of pupil: _____

When I use a computer, tablet or the internet at school:

- I will ask an adult and follow their instructions.
- I will use my own login and keep my password private.
- I will be kind to people online.
- I will look after the equipment.
- I will only use websites, apps and AI tools my teacher says I can use.
- I will tell an adult straight away if I see something that worries or upsets me.
- I will ask before taking or sharing a photo or video.
- I will remember that things I see online or things AI tells me might not always be true.
- I will not try to get around the school's safety settings.

I understand that adults may check how school computers and accounts are being used to help keep everyone safe.

Pupil signature: _____ Date: _____

Parent/carer: I have discussed these rules with my child and support the school's approach to safe technology use.

Parent/carer signature: _____ Date: _____

Appendix 5: Acceptable use agreement for staff, governors, volunteers, contractors and visitors

Name: _____

Role: _____

I understand that access to school and Trust digital technology is provided for authorised purposes and that safeguarding, confidentiality and professional conduct apply to my use.

I agree that I will:

- use only accounts, devices, systems and services I am authorised to use;
- keep passwords and authentication information secure;
- lock devices when unattended and protect confidential information from unauthorised access;
- use approved school/Trust systems for school business and personal data;
- report safeguarding concerns to the DSL and technical/cyber concerns through the appropriate Trust IT route;
- report actual or suspected data breaches immediately;
- follow school and Trust requirements for email, remote access, personal devices and social media;
- maintain professional boundaries with pupils and families;
- use AI responsibly, transparently and in accordance with section 10 of this policy;
- not enter personal, safeguarding or confidential information into unapproved AI systems;
- not bypass filtering, monitoring, security or device-management controls;
- not install unauthorised software or connect unauthorised equipment;
- respect copyright, privacy and intellectual property;
- return school/Trust equipment and cease access when my role or authorisation ends.

I understand that use of school and Trust systems may be monitored lawfully and proportionately for safeguarding, security, compliance and operational purposes.

Signed: _____ Date: _____

Authorising member of staff (where required): _____

Approval

Headteacher	
Chair of Local Governing Body	
Date approved	
Effective date	1 September 2026
Next formal review	January 2028

Key national references used in preparing this policy: Keeping Children Safe in Education 2026; DfE Filtering and Monitoring Standards; DfE Cyber Security Standards; DfE Generative AI in Education guidance and Generative AI Product Safety Standards. The policy should be kept aligned with current St Thomas Aquinas Catholic Multi-Academy Trust policies and technical arrangements.