

Acceptable Use Policy

St Matthew's Catholic Primary School

Love, Learn and Shine together with Jesus



Safe, responsible and lawful use of technology 2026 to 2027

Approved by	Governing Body
Policy owner	Headteacher and Designated Safeguarding Lead
Approval date	September 2026
Review date	September 2027, or sooner if guidance or practice changes
Status	Supports statutory safeguarding, data-protection and curriculum duties

1 Purpose and scope

Technology supports teaching, learning, communication and school administration. This policy sets the conditions under which pupils, staff, governors, volunteers, contractors and visitors may use school devices, networks, accounts, platforms and data. It applies on and off site whenever school technology, accounts or information are used.

Access to school technology is a privilege and carries responsibilities. Users must protect children, respect others, safeguard information and use technology only for lawful and authorised purposes.

2 Core expectations for every user

- Use school technology for education, school business or another purpose authorised by the Headteacher.
- Use only an individual account and keep passwords and multifactor authentication details private.
- Treat others respectfully and never use technology to bully, harass, threaten, discriminate, humiliate or impersonate another person.
- Do not create, access, store or share illegal, sexual, violent, hateful, extremist or otherwise harmful material.
- Do not try to bypass filtering, monitoring, security controls or access restrictions, including through a VPN, proxy, personal hotspot or unauthorised account.
- Do not install software, browser extensions, applications or devices without approval.
- Protect personal, special-category and confidential information and share it only through approved systems with authorised people.
- Immediately report accidental access, suspicious messages, data loss, cyber incidents or online-safety concerns. Pupils tell a trusted adult; adults report safeguarding concerns to the DSL and record them on CPOMS where required.
- Understand that school systems are filtered and monitored. Users must not expect personal privacy when using them, although monitoring will be lawful, proportionate and limited to authorised purposes.

3 Unacceptable use

Unacceptable use includes, but is not limited to:

- accessing, producing or distributing material that is illegal, pornographic, abusive, discriminatory, defamatory or harmful;
- making, requesting, possessing or sharing nude or semi-nude images, sexualised deepfakes or other child sexual abuse material;
- cyberbullying, hate speech, sexual harassment, grooming, coercion, financial abuse or encouraging self-harm or suicide;
- unauthorised recording, photography, livestreaming, location sharing or publication of information about pupils, staff or the school;
- using another person's account, disclosing passwords, hacking, scanning, introducing malware or damaging or disrupting systems;
- online gambling, unauthorised purchasing, cryptocurrency activity, phishing, scams or commercial activity;
- infringing copyright, licence terms or intellectual-property rights, or presenting another person's or AI-generated work dishonestly;
- using school systems to bring the school into disrepute or to disclose confidential information; and
- using personal email, messaging, cloud storage or social-media accounts for school records or communication with pupils.

4 Staff, governors, volunteers and contractors

Adults must model professional behaviour and comply with the Staff Code of Conduct, Child Protection and Safeguarding Policy, Data Protection Policy, AI Policy and instructions from the Headteacher, DSL, DPO and authorised IT support.

- Use school-approved accounts and devices for school business. Lock devices when unattended and store them securely.
- Communicate with pupils and families only through approved school channels. Do not accept or initiate personal social-media connections with current pupils.
- Do not use a personal device to photograph, film or record pupils. School images must be taken on an approved school device and transferred promptly to approved storage.
- Do not publish names with images or disclose a pupil's location, timetable, needs or other identifying information unless specifically authorised.
- Check recipients before sending messages or files, use Bcc when appropriate and report misdirected information immediately to the DPO.
- Do not access personal or sensitive information unless it is necessary for the role.
- Supervise pupils' technology use actively. Filtering and monitoring do not replace adult supervision.
- Report safeguarding concerns immediately to the DSL and record them on CPOMS. Report suspected data breaches to Mrs Louisa Chamberlain, DPO, without delay.
- Return school equipment and information when requested or when employment or engagement ends.

5 Generative artificial intelligence

Only AI services approved by the school may be used. Staff have access to the school-approved Google Gemini platform and Chalkie AI to support teaching and planning. Approval does not remove the user's professional responsibility.

- Never enter pupil names, photographs, voices, work containing identifiers, safeguarding information, medical information, SEND records, staff personal data, passwords or any confidential school information into an AI system.
- Pupil photographs or other images of identifiable children must never be uploaded to generative AI or image-manipulation services.
- Check all AI output for accuracy, bias, suitability, copyright and safeguarding risk before use. AI must not make final professional, safeguarding, assessment, admission, behaviour, employment or SEND decisions.
- Acknowledge material AI use where appropriate. AI must not be used to deceive, plagiarise, impersonate, fabricate evidence or create harmful or sexualised deepfakes.
- Pupils may use AI only when a teacher has approved the tool and activity, age restrictions are met and close supervision and appropriate safeguards are in place.

6 Pupils

Rules are taught in age-appropriate language. Pupils must use only the account and device provided or approved for them, follow staff instructions and tell an adult if anything online worries, upsets or confuses them. They must not share passwords or personal information, contact strangers, bypass controls, make secret recordings or upload images of others without permission.

Only Year 6 pupils who walk home independently and have written permission may bring a mobile phone. It must be handed in on arrival, stored securely and collected at the end of the day. It must not be used on the school site unless a member of staff gives specific permission. Agreed medical or SEND arrangements will be recorded separately.

7 Images, video and audio

The school will use images only where there is a clear educational or communication purpose and an appropriate lawful basis. Consent choices will be respected. To reduce identification and AI-manipulation risks, external publications will normally use partial, group, distant or rear-view images rather than clear, high-resolution full-face photographs. Images will not normally be paired with a child's full name.

Parents and carers may be asked not to photograph or record at particular events. Images taken for personal use must not be posted or shared where other children can be identified without permission.

8 Data and cyber security

- Use strong, unique passwords and multifactor authentication where available; never approve an unexpected login request.
- Store school information only in approved locations; do not transfer it to personal email, unapproved cloud storage or removable media.
- Apply updates promptly and do not disable antivirus, encryption, filtering or device-management controls.
- Treat unexpected links, attachments, payment requests and changes of bank details as suspicious and verify them independently.
- Immediately report lost devices, malware, unauthorised access, accidental disclosure or suspected compromise. Do not attempt an investigation that may destroy evidence.

9 Filtering, monitoring and privacy

The school uses NfGL filtering and monitoring to restrict harmful content and identify concerning activity. Authorised members of the safeguarding team receive and review alerts, which may be checked against the IP address and device information. The school may lawfully inspect activity, communications and files on its systems for safeguarding, security, compliance and operational purposes.

Monitoring is not continuous outside school hours and cannot guarantee that all harmful content will be blocked. Any urgent concern must be reported directly to the school, police or emergency services as appropriate.

10 Breaches and response

Concerns will be considered according to their nature, seriousness, intent, impact, age and any SEND or vulnerability. The school may preserve evidence; restrict or remove access; contact parents, the DPO, IT support, LADO, local authority, police or other agencies; and use its Behaviour, Staff Disciplinary, Complaints or Safeguarding procedures. Illegal material must not be copied, printed, forwarded or unnecessarily viewed.

11 Responsibilities and review

Role	Main responsibilities
Governing Body	Approves the policy and assures itself that safeguarding, filtering, monitoring and cyber-security arrangements are effective.
Headteacher and DSL	Leads implementation, responds to safeguarding concerns and decides proportionate action.
DPO – Mrs Louisa Chamberlain	Advises on data protection and manages suspected personal-data breaches.
IT support	Maintains systems, accounts, security, filtering and monitoring and provides reports and technical advice.
All adults	Follow the policy, supervise pupils, protect information and report concerns promptly.
Pupils and families	Follow the relevant agreement and report concerns or accidental access.

The policy and associated agreements will be reviewed at least annually and after a significant incident, system change or change in legislation or guidance.

12 Related school policies

- Child Protection and Safeguarding Policy
- Online Safety Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy and Privacy Notices

- AI Policy
- Mobile Phone Policy
- Safe Use of Children's Photographs Policy
- Anti-Bullying Policy
- Searching, Screening and Confiscation arrangements
- Whistleblowing and disciplinary procedures

Appendix 1 Staff and adult acceptable use agreement

I confirm that I have read and will follow this policy. In particular, I will use approved systems, maintain professional boundaries, protect confidential information, never use a personal device to record pupils, never upload identifiable pupil information or images to generative AI, supervise pupils and report concerns immediately.

Name: _____ Role: _____

Signature: _____ Date: _____

Appendix 2 Pupil acceptable use agreement

- I use technology only when an adult says I may.
- I keep my password and personal information private.
- I am kind and respectful online.
- I do not take or share photographs, videos or recordings without permission.
- I do not try to get around school safety controls.
- I tell a trusted adult straight away if I see something worrying, upsetting or unsafe.
- I understand that the school checks how its devices and accounts are used.

Pupil name: _____ Class: _____

Pupil signature: _____ Date: _____

Parent or carer signature: _____ Date: _____

Key legislation and guidance

This policy should be read alongside the school's Child Protection and Safeguarding Policy and the related school policies listed below. It has regard to:

- Keeping Children Safe in Education 2026 (statutory guidance).
- Data Protection Act 2018 and UK General Data Protection Regulation.
- Data (Use and Access) Act 2025.
- Computer Misuse Act 1990; Copyright, Designs and Patents Act 1988; Human Rights Act 1998; Equality Act 2010.
- DfE Filtering and Monitoring Core Standard and Cyber Security Core Standard.
- DfE Generative Artificial Intelligence in Education and Generative AI Product Safety Standards.
- DfE Mobile Phones in Schools guidance and Searching, Screening and Confiscation advice.
- Statutory Relationships Education, Relationships and Sex Education and Health Education guidance.