



St Michael & St Martin Catholic Primary School

IT Acceptable Use Policy

Purpose and scope

This policy sets rules for safe, secure and professional use of school technology and information. It applies to school devices, accounts, networks, Wi-Fi and data, including authorised remote access and any approved personal-device access. It covers staff, governors, pupils, volunteers, supply staff, contractors and visitors according to their access.

Users must receive the rules relevant to their role and agree to them before access is enabled. The school records acknowledgement and provides support where needed. Pupil rules are explained in age-appropriate language; younger children use technology under adult supervision.

Core rules for all users

- Use only accounts and access granted to you. Do not share passwords, use another person's account, attempt unauthorised access or bypass security or filtering.
- Use technology respectfully and lawfully. Do not create, access or share abusive, discriminatory, threatening, exploitative, sexually inappropriate or otherwise harmful material.
- Protect personal information and confidential school material. Access, share and store only what is necessary for your authorised purpose.
- Use approved software, storage and communication services. Do not install software, connect storage devices or change security settings without authorisation.
- Report harmful content, mistakes, suspicious messages, lost equipment and suspected misuse promptly. Seeking help is encouraged; hiding an incident can increase harm.

Administration and review

The digital lead works with the DSL, DPO and IT support to maintain this policy and approved-system arrangements. Staff and governor acknowledgements are reviewed annually and after material changes. Pupil agreements are revisited at the beginning of each academic year. Visitor and contractor access is time-limited and proportionate.

Professional use and information security

Accounts and devices

- Use strong, unique passwords and approved password-management arrangements. Enable multi-factor authentication where required. Never approve an unexpected authentication request.
- Lock screens when leaving devices, keep equipment secure and apply updates as directed. Report faults; do not disable protective software.
- Do not send school information to personal email or store it in personal cloud accounts. Access confidential information remotely only through approved secure arrangements.
- Report lost or stolen devices immediately. School equipment remains subject to school security requirements when taken home. Return equipment and cease account access when your role ends.
- Personal devices may access school data only where specifically authorised, risk assessed and protected. An exception must not override the school mobile phone or EYFS rules.

Email and electronic communication

Use approved school channels for work communications with pupils and families. Check recipients and attachments, use secure sharing for sensitive information and avoid unnecessary personal information. Verify unexpected requests for payments, bank-detail changes or credentials through an independently obtained contact route.

Staff must maintain professional boundaries, including outside working hours. Do not use personal social media accounts or private messaging to communicate with pupils. Remote lessons and meetings must use authorised platforms and appropriate access controls.

Social media photography and recording

Only authorised users may post on school accounts. Posts must respect confidentiality, copyright, image permissions and safeguarding. Personal posts must not disclose confidential school information or undermine professional boundaries. Concerns are raised through appropriate school processes.

Take and store school photographs and recordings only using approved equipment and systems for an authorised purpose. Check the relevant permissions, lawful basis and restrictions before publication. Do not upload pupil images to personal accounts, messaging services or unapproved AI tools.

Personal use

Any limited personal use of school technology requires school permission, must not disrupt work or pupil supervision, and must comply with this policy. The school may restrict personal use to protect safety, security and resources.

Monitoring AI and breaches of this policy

Monitoring and privacy

The school operates filtering and monitoring to protect pupils and systems. Depending on the confirmed services, authorised staff may review network activity, alerts and relevant account or device records for safeguarding, security or other lawful school purposes. Access is limited, proportionate and recorded where appropriate. Monitoring details, retention and users' rights are explained in privacy notices and the Online Safety Policy.

Users should not assume school systems are private. This does not authorise unrestricted surveillance. The school explains significant changes to monitoring and assesses privacy risks with the DPO. Technical monitoring does not guarantee that every harmful action will be detected.

AI acceptable use rules

- Use only AI tools approved for the intended task. Approval must consider age restrictions, safeguarding, privacy, security, copyright, accessibility and how prompts and outputs are retained or used by the supplier.
- Do not enter identifiable pupil, family or staff information, safeguarding records, SEND or medical information, personnel records or confidential governor papers into general-purpose AI tools. Any exceptional personal-data use requires prior documented approval and DPO review of the lawful basis, safeguards and any required DPIA.
- Remove identifying details and consider whether a person could still be identified from context. Merely removing a name may not anonymise information.
- Check outputs for accuracy, bias, suitability and copyright concerns before use. A responsible member of staff retains judgement and accountability. AI must not make final safeguarding, assessment, disciplinary or employment decisions.
- Pupil-facing use requires prior approval, suitable supervision and compliance with provider age limits and terms. Pupils must not create accounts independently for school tasks.
- Do not use AI to impersonate people, fabricate evidence or create harmful imagery. Explain substantial AI assistance where transparency is relevant to the task.

Reporting and consequences

Report safeguarding concerns directly to the DSL or deputy; technical incidents to IT support and the Headteacher; and possible personal data breaches immediately to the Headteacher and DPO. Do not wait until you can prove an incident. Access may be restricted while risk is assessed. Responses consider age, intent, impact and vulnerability and may involve education, behaviour procedures, disciplinary action or external referral as appropriate.

Guidance and related documents

DfE cyber security standard

DfE filtering and monitoring standard

DfE generative AI guidance

Read alongside the school Child Protection and Safeguarding Policy, Staff Code of Conduct, Behaviour Policy, Mobile Phone Policy and the other school IT policies