



ICT AND INTERNET ACCEPTABLE USE POLICY

Policy date: September 2026
Review date: September 2029
Approved by: Governing Body

1. INTRODUCTION

Information and communication technology (ICT) is an integral part of life at St Mary's R.C. Primary School. ICT supports teaching and learning, communication, administration, safeguarding and the effective operation of the school.

The school provides access to computers, laptops, tablets, the internet, email, online services, applications and other digital technologies to support the school's educational and operational aims.

The school is committed to ensuring that ICT is used safely, responsibly and appropriately.

This policy sets out the expectations for the acceptable use of the school's ICT facilities and internet access. It is intended to:

- promote the safe, responsible and effective use of technology;
- protect pupils, staff and other users from online risks;
- support safeguarding and online safety;
- protect school systems, equipment and information;
- support compliance with data protection and other legal requirements;
- prevent misuse of ICT facilities;
- promote respectful and appropriate online behaviour;
- ensure that users understand their responsibilities when using school ICT facilities.

This policy applies to:

- pupils;
- teaching and support staff;
- governors;
- volunteers;
- contractors;
- visitors;
- parents/carers when using school ICT facilities; and
- any other person authorised to access school systems.

Failure to comply with this policy may result in access being restricted or withdrawn and may lead to disciplinary, behaviour or other appropriate action.

2. SCOPE

This policy applies to the use of:

- school computers and laptops;
- tablets and iPads;
- mobile phones and other mobile devices;
- school networks and Wi-Fi;
- internet access;
- school email;
- online learning platforms;
- cloud services;
- software and applications;

- school websites and social media accounts;
- remote access systems;
- removable storage devices;
- online communication and collaboration tools;
- generative artificial intelligence (AI) tools; and
- any other ICT system or digital technology provided or authorised by the school.

The policy applies whether equipment or systems are being used on school premises, remotely or at another location on behalf of the school.

3. LEGISLATION AND GUIDANCE

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

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- 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;
- Keeping Children Safe in Education 2026;
- Department for Education guidance on filtering and monitoring;
- Department for Education guidance on searching, screening and confiscation;
- Department for Education guidance on mobile phones in schools; and
- Prevent Duty guidance.

KCSIE 2026 requires schools to maintain appropriate safeguarding arrangements, including appropriate filtering and monitoring of online activity.

The DfE's filtering and monitoring standard requires schools to review their provision at least annually, assign clear responsibilities, maintain effective monitoring arrangements and record actions arising from reviews.

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy;
 - Online Safety Policy;
 - Data Protection Policy;
 - Behaviour Policy;
 - Mobile Phone Policy;
 - Cyber Security arrangements;
 - Staff Code of Conduct;
 - Social Media Policy/guidance; and
 - Complaints Policy, where appropriate.
-

4. DEFINITIONS

ICT facilities - ICT facilities include the school's network infrastructure, computers, laptops, tablets, iPads, mobile devices, telephones, software, applications, websites, online services, cloud services, learning platforms and any other current or future ICT system provided or authorised by the school.

Users - Users are anyone authorised to use the school's ICT facilities, including staff, pupils, governors, volunteers, contractors and visitors.

Personal use

Personal use means activity that is not directly related to a user's employment, education, volunteering or authorised purpose within the school.

Authorised personnel - Authorised personnel are individuals who have been given permission to administer, maintain, monitor or support the school's ICT systems.

Materials

Materials include electronic files, documents, photographs, audio, video, printed information, websites, online content, social media posts, messages and other digital information.

5. ACCEPTABLE USE

Users must:

- use school ICT facilities responsibly and appropriately;
- use systems only for authorised purposes;
- respect other users;
- protect passwords and account information;
- follow school safeguarding and online safety procedures;
- report inappropriate, harmful or suspicious content;
- report suspected cyber security incidents;
- respect copyright and intellectual property;
- protect confidential school information;
- follow the school's Data Protection Policy;
- use school equipment carefully;
- follow staff instructions regarding the use of technology;
- comply with filtering and monitoring arrangements; and
- immediately report accidental access to inappropriate or restricted material.

6. UNACCEPTABLE USE

Users must not use school ICT facilities to:

- access, create, download, store or distribute illegal, pornographic, abusive, discriminatory, offensive or otherwise inappropriate material;
- bully, harass, threaten or intimidate another person;
- send or post material that is discriminatory, offensive or defamatory;
- bring the school into disrepute;
- share confidential or personal information without appropriate authorisation;
- access another person's account or files without permission;

- attempt to bypass or disable filtering, monitoring or other security systems;
- install software, applications or browser extensions without authorisation;
- connect unauthorised devices or equipment to the school network;
- deliberately introduce viruses, malware or other harmful software;
- damage, alter or interfere with school equipment or systems;
- delete or alter information without authorisation;
- attempt to gain unauthorised access to systems or networks;
- use another person's username or password;
- undertake illegal activity;
- infringe copyright or other intellectual property rights;
- conduct unauthorised commercial or private business activities;
- use school systems to promote personal political, commercial or other inappropriate activities;
- access gambling or inappropriate gaming sites;
- deliberately access material blocked by the school's filtering system;
- use technology to facilitate abuse or exploitation of others; or
- undertake any activity that could compromise the safety, security or reputation of the school.

This list is not exhaustive. The Headteacher or designated senior leader will determine whether particular use is appropriate.

7. STAFF, GOVERNORS, VOLUNTEERS AND CONTRACTORS

All staff, governors, volunteers and contractors are responsible for ensuring that their use of ICT complies with this policy.

Users will be provided with individual accounts where appropriate.

Users must:

- keep passwords confidential;
- never use another person's account;
- lock their device when unattended;
- log out when finished;
- ensure confidential information is not visible to unauthorised individuals;
- report suspected security incidents promptly;
- follow school procedures when handling personal data;
- use school email accounts for school business where appropriate;
- exercise professional judgement when communicating electronically; and
- maintain professional boundaries when communicating with pupils and parents.

Access rights will be provided according to the user's role and responsibilities.

Requests for new or amended access should be made through the appropriate school procedures.

8. EMAIL AND ELECTRONIC COMMUNICATION

School email accounts should be used for school business.

Staff must not normally use personal email accounts to communicate with pupils or parents about school matters.

Staff must:

- check recipients carefully before sending messages;
- use professional and appropriate language;
- avoid including unnecessary personal information;
- consider whether attachments contain confidential information;
- use appropriate security measures when sending sensitive information;
- report emails sent to the wrong recipient immediately;
- report suspected phishing or malicious emails; and
- retain or delete emails in accordance with school procedures.

If personal data is sent to the wrong person, this must be reported immediately in accordance with the school's Data Protection Policy and data breach procedures.

Staff should not provide pupils or parents with their personal telephone number or use personal messaging services for routine school communication unless specifically authorised by the school.

9. PERSONAL USE OF SCHOOL ICT

Limited personal use of school ICT may be permitted at the Headteacher's discretion, provided that it:

- does not interfere with work;
- does not take place during teaching or other duties;
- does not involve pupils being present;
- does not breach this policy;
- does not create additional security risks;
- does not involve inappropriate content; and
- does not involve the storage or processing of unauthorised personal information.

The school reserves the right to withdraw permission for personal use.

10. PERSONAL DEVICES AND BRING YOUR OWN DEVICE (BYOD)

Personal devices must not be connected to the school's network unless specifically authorised.

Where personal devices are authorised, users must comply with the school's security requirements. Access to the Network is via the Guest wifi login details.

Users must not use personal devices to:

- photograph or record pupils without appropriate authorisation;

- store confidential school information without authorisation;
- access school systems without appropriate security;
- communicate inappropriately with pupils;
- bypass school filtering or monitoring; or
- undertake activities that could compromise school systems.

The school may restrict or prohibit the use of personal devices where there is a safeguarding, security or operational concern.

11. MOBILE PHONES

The use of mobile phones by pupils will be managed in accordance with the school's Mobile Phone Policy and current Department for Education requirements.

Pupils must not use mobile phones during the school day.

Staff should follow the school's expectations regarding personal mobile phone use.

Personal mobile phones must not be used to photograph, video or record pupils unless specifically authorised for a legitimate school purpose.

School-owned mobile phones must be used appropriately and securely.

The Department for Education's statutory mobile phone guidance came into force on 29 June 2026 and schools should follow it from 1 September 2026.

12. INTERNET ACCESS

The school's internet access is provided primarily for educational and operational purposes.

Users must:

- use the internet responsibly;
- follow school filtering arrangements;
- report inappropriate content;
- report websites that should reasonably be blocked;
- report websites that have been incorrectly blocked where this affects legitimate teaching or school business; and
- follow staff instructions regarding internet use.

Users must not attempt to bypass or disable filtering.

The school recognises that no filtering system can guarantee that all harmful or inappropriate content will be blocked. Filtering therefore forms part of a wider safeguarding approach which includes monitoring, education, supervision and reporting procedures.

13. FILTERING AND MONITORING

The school has appropriate filtering and monitoring systems in place to help protect pupils and staff from harmful, inappropriate and illegal online content.

Filtering - Filtering is used to prevent access to inappropriate or harmful online content.
Monitoring

Monitoring is used to identify potentially harmful activity, safeguarding concerns, inappropriate use, cyber security incidents and other risks.

The school's filtering and monitoring arrangements will:

- apply to school-managed devices and systems;
- be appropriately configured and maintained;
- be reviewed at least annually;
- be reviewed following significant changes to technology or identified risks;
- include consideration of remote access and personal devices where applicable;
- provide appropriate alerts or reports;
- support safeguarding responses;
- record significant incidents and actions taken; and
- be reviewed following significant system or equipment changes.

The DfE currently expects schools to have clear roles and responsibilities for filtering and monitoring, undertake an annual review involving senior leadership, the DSL, IT support and the responsible governor, and record the outcome and actions.

The school's IT provider will support the technical management of filtering and monitoring.

The Designated Safeguarding Lead (DSL) will be involved where monitoring identifies a safeguarding concern.

Staff and other users will be informed that school ICT systems may be monitored.

Monitoring will be carried out proportionately and in accordance with applicable data protection requirements.

14. MONITORING REPORTS AND SAFEGUARDING ALERTS

The school's monitoring arrangements will include appropriate procedures for responding to alerts.

Monitoring reports and alerts will be reviewed by appropriately authorised personnel.

High-risk safeguarding, malicious or technical incidents will be escalated promptly.

Where an alert relates to a pupil and raises a safeguarding concern, it will be referred to the DSL or another appropriate safeguarding member of staff.

The school will record significant incidents, actions taken and outcomes where appropriate.

The DfE's current standard recommends, as a minimum, weekly monitoring reports highlighting incidents and immediate reporting of high-risk incidents.

15. GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

Generative AI tools must only be used where authorised by the school and for appropriate educational or operational purposes.

Users must not:

- enter personal, confidential or sensitive information about pupils, parents, staff or other individuals into an AI tool unless specifically authorised and appropriate safeguards are in place;
- use AI to create inappropriate, discriminatory, harmful or offensive content;
- rely on AI-generated information without checking its accuracy;
- use AI in a way that breaches copyright or intellectual property rights; or
- use AI to make safeguarding or other significant decisions without appropriate human oversight.

AI-generated content must be checked for:

- accuracy;
- appropriateness;
- bias;
- safeguarding concerns;
- reliability; and
- potential data protection issues.

Pupils may only use generative AI tools where permitted by staff and in accordance with curriculum and online safety arrangements.

The school will consider the safeguarding and data protection implications of any generative AI tools it introduces. Current DfE guidance specifically requires schools to consider AI-generated content when reviewing filtering and monitoring arrangements.

16. PASSWORDS AND ACCOUNT SECURITY

Users must:

- use strong passwords;
- keep passwords confidential;
- never share passwords with other users;
- not write passwords where they can be easily accessed;
- change passwords when instructed;
- use multi-factor authentication where provided;
- lock devices when unattended; and
- report suspected compromised accounts immediately.

Users are responsible for activity carried out using their account unless they have reported that their account has been compromised.

17. CYBER SECURITY

All users have a responsibility to help protect the school against cyber threats.

Users must:

- be cautious when opening unexpected emails or attachments;
- not click suspicious links;
- report suspected phishing;
- not install unauthorised software;
- not disable security controls;
- keep school devices secure;
- follow instructions relating to software and security updates;
- report lost or stolen school devices immediately; and
- report suspected viruses, malware or other security incidents immediately.

The school will maintain appropriate technical safeguards and work with its IT provider to support cyber security.

18. DATA PROTECTION AND CONFIDENTIALITY

The school is committed to protecting personal and confidential information.

Users must handle personal data appropriately and securely.

Personal data must only be accessed, used, stored or shared where there is an appropriate school-authorised purpose.

Users must follow the school's **Data Protection Policy**.

This policy does not replace the school's Data Protection Policy or detailed data protection procedures.

Users must immediately report suspected data breaches in accordance with the school's data breach procedures.

The Data (Use and Access) Act 2025 amended and built on the existing UK GDPR and Data Protection Act 2018 framework, with relevant changes coming into force during 2026.

19. REMOTE ACCESS

Remote access to school systems may be provided to authorised staff where required for their role.

Remote access must:

- use school-approved systems;
- use individual user credentials;
- use appropriate security measures;
- be carried out using a secure internet connection;
- follow the same rules as access within school;

- protect confidential information from unauthorised access; and
- comply with the school's Data Protection Policy.

Users must take particular care when accessing school information in public places or on shared devices.

20. SOCIAL MEDIA AND ONLINE COMMUNICATION

Staff, governors, volunteers and contractors should maintain professional boundaries when using social media.

Users must not:

- communicate with pupils through personal social media accounts;
- accept pupils as personal social media contacts where this would create an inappropriate professional relationship;
- post confidential school information;
- post photographs or videos of pupils without appropriate authorisation;
- make inappropriate comments about pupils, parents, colleagues or the school;
- disclose information that could identify or place a child at risk;
- use social media to bully, harass or discriminate against others; or
- bring the school into disrepute.

Staff should remember that information posted online may remain accessible even after deletion.

Personal social media activity that raises safeguarding, professional conduct or reputational concerns may be addressed through the school's appropriate procedures.

21. PUPIL USE OF ICT

Pupils will be taught to use technology safely, responsibly and respectfully. Pupils must:

- follow staff instructions;
- use school devices appropriately;
- use their own accounts;
- keep passwords secure;
- treat equipment with care;
- use appropriate language;
- respect other people's privacy;
- report anything that makes them feel worried or uncomfortable;
- report inappropriate content;
- not attempt to bypass filtering;
- not access another person's account;
- not deliberately damage equipment; and
- not use technology to bully, threaten or harm others.

Pupils should be encouraged to follow the principle:

“If you would not say or do it face-to-face, do not say or do it online.”

22. SEARCHING AND CONFISCATION OF DEVICES

The school may search, screen and confiscate devices or other items where permitted by law and in accordance with the school's Behaviour Policy and the Department for Education's guidance on **Searching, Screening and Confiscation**.

Searches will be carried out by authorised staff and in accordance with the relevant legal requirements and school procedures.

A parent does **not** need to be present as a general condition of a lawful school search.

Where a pupil's device is searched, staff will consider the pupil's privacy and the nature of the concern.

Any safeguarding concerns identified during a search will be dealt with under the school's safeguarding procedures.

The school's current searching arrangements will follow the DfE guidance, which sets out schools' powers to search pupils and confiscate items found.

23. SCHOOL EQUIPMENT

Users are responsible for taking reasonable care of school ICT equipment. Users must not:

- deliberately damage equipment;
- remove equipment without permission;
- alter hardware without authorisation;
- interfere with cables or network equipment;
- install unauthorised software;
- attempt to repair equipment unless authorised; or
- use equipment for inappropriate purposes.

Faults should be reported to the appropriate member of staff.

24. PARENTS, CARERS AND VISITORS

Parents, carers and visitors will not normally be given access to school ICT systems.

Where access is required for an authorised school purpose, such as volunteering, governance or an agreed presentation, access may be provided at the school's discretion to the Guest wifi password.

Parents, carers and visitors must:

- follow staff instructions;
- use systems only for the authorised purpose;
- respect confidentiality;
- not access information belonging to pupils or staff;
- not photograph or record pupils without permission; and
- use respectful and appropriate communication.

The school expects parents and carers to model positive and respectful online behaviour.

Concerns about the school should be raised through the appropriate school communication or complaints procedure rather than through inappropriate online posts.

25. INCIDENT REPORTING

All users must report concerns promptly. Examples include:

- inappropriate or harmful online content;
- cyber bullying;
- suspected online abuse;
- suspicious emails;
- phishing;
- malware or viruses;
- lost or stolen equipment;
- compromised passwords;
- accidental access to confidential information;
- data breaches;
- attempts to bypass filtering;
- inappropriate use of school systems; and
- safeguarding concerns arising from online activity.

Reports should be made to the Headteacher, Deputy Headteacher, DSL, Business Manager, depending on the nature of the incident.

Safeguarding concerns must be reported immediately in accordance with the Child Protection and Safeguarding Policy.

26. CONSEQUENCES OF MISUSE

Misuse of ICT facilities may result in:

- removal or restriction of ICT access;
- removal of internet access;
- confiscation of equipment where permitted;
- behaviour sanctions for pupils;
- disciplinary action for staff;
- referral to safeguarding procedures;
- referral to the police or other external agencies where appropriate; and/or
- other action considered necessary by the school.

The response will be proportionate to the nature and seriousness of the incident.

27. ROLES AND RESPONSIBILITIES

Governing Body - The Governing Body will:

- provide strategic oversight of ICT and online safety;
- ensure appropriate policies are in place;
- receive appropriate assurance regarding filtering and monitoring;
- ensure filtering and monitoring arrangements are reviewed at least annually; and
- challenge and support the school where necessary.

Headteacher – The Headteacher will:

- oversee implementation of this policy;
- ensure staff understand their responsibilities;
- ensure appropriate systems are in place;
- work with the DSL and IT provider;
- take appropriate action where the policy is breached; and
- ensure the policy is reviewed regularly.

Designated Safeguarding Lead - The DSL will:

- oversee safeguarding concerns arising from online activity;
- respond to relevant filtering and monitoring alerts;
- ensure online safeguarding concerns are recorded and managed appropriately;
- work with IT support and senior leaders; and
- ensure online safety remains part of the school's wider safeguarding arrangements.

IT Support / IT Provider - The school's IT provider will:

- support the secure operation of school systems;
- maintain appropriate technical safeguards;
- support filtering and monitoring;
- provide technical advice;
- support system updates and security;
- assist with incident investigation; and
- escalate significant technical or security concerns.

Staff - staff will:

- follow this policy;
- supervise pupils appropriately;
- use technology responsibly;
- protect school information;
- report incidents and safeguarding concerns;
- follow filtering and monitoring procedures; and
- undertake relevant ICT, online safety and cyber security training.

Pupils - Pupils will:

- use ICT safely and responsibly;
- follow school rules;
- respect others online;
- protect their passwords;
- report concerns; and
- follow staff instructions.

28. TRAINING AND AWARENESS

The school will provide appropriate training and guidance to staff.

Training will cover relevant areas including:

- online safety;
- safeguarding;
- data protection;
- cyber security;
- phishing and other online threats;
- appropriate use of school systems;
- filtering and monitoring;
- social media;
- mobile devices; and
- generative AI where relevant.

The school will ensure that staff are aware of how to report concerns and how filtering and monitoring alerts are managed.

29. MONITORING AND REVIEW OF THIS POLICY

This policy will be reviewed **at least annually**. It will also be reviewed sooner where there are:

- changes to legislation;
- changes to statutory guidance;
- significant changes to technology;
- changes to filtering or monitoring systems;
- changes to school procedures;
- new cyber security risks;
- introduction of new digital or AI technologies; or
- significant safeguarding concerns.

The DfE's current digital and technology standards identify filtering and monitoring and cyber security as core areas for schools, alongside broadband, wireless, network switching and digital leadership/governance.

The outcome of the annual review will be reported through the school's appropriate governance arrangements.

30. RELATED POLICIES AND DOCUMENTS

This policy should be read alongside:

- Child Protection and Safeguarding Policy;
- Online Safety Policy;
- Data Protection Policy;
- Behaviour Policy;
- Mobile Phone Policy;
- Staff Code of Conduct;
- Cyber Security procedures;
- Social Media guidance;
- Complaints Policy;
- Records Management procedures; and
- Filtering and Monitoring arrangements.