

Sele First School

Acceptable Use Policy 2026 - 2027

Staff, Volunteers, Governors, Contractors and Visitors

Related Policies:

Safeguarding and Child Protection Policy
Online Safety Policy
Staff Code of Conduct
Data Protection Policy
Relational Behaviour Policy
UK GDPR and Data Protection procedures
DfE Keeping Children Safe in Education (KCSIE) 2026
DfE Filtering and Monitoring Standards for Schools and Colleges
DfE Generative Artificial Intelligence (AI) Guidance for Schools and Colleges

Introduction

Digital technologies, online services and artificial intelligence (AI) systems are integral to teaching, learning, communication and school operations. This Acceptable Use Policy (AUP) is intended to ensure that all staff, volunteers, governors, contractors and visitors use technology safely, responsibly, professionally and in accordance with current legislation and Department for Education (DfE) guidance.

Sele First recognises that the internet and digital technologies provide significant educational benefits; however, they also present safeguarding, data protection, cybersecurity and reputational risks.

All users are expected to:

- Use technology safely, legally and professionally.
- Safeguard pupils and colleagues online.
- Protect confidential and personal data.
- Follow school policies and procedures.
- Report concerns, incidents or breaches immediately.
- Use AI tools responsibly and in accordance with school guidance.

This policy applies to all use of:

- School devices and systems
- Personal devices used on school premises or for school business
- School networks and Wi-Fi
- Remote access systems

- Cloud-based services and applications
- Email systems
- Artificial intelligence tools and platforms
- Social media and online communication

All staff must read and sign this policy annually.

School Digital Strategy and Security Measures

Sele First employs a range of technical and organisational measures to maximise learning opportunities and minimise risks associated with digital technologies.

These include:

- Filtering and monitoring systems compliant with DfE filtering and monitoring standards.
- Endpoint protection and anti-malware software.
- Secure user authentication and multi-factor authentication (MFA).
- Network monitoring and logging.
- Restricted administrative access.
- Regular cybersecurity updates and patching.
- Secure cloud-based storage systems.
- Staff training in safeguarding, online safety, data protection and cybersecurity.

Sele First reserves the right to monitor use of school systems, devices and internet access where lawful and proportionate to ensure:

- Safeguarding of pupils and staff
- Compliance with school policies
- Network security
- Prevention and detection of misuse
- Compliance with legal obligations

Monitoring will be conducted in accordance with UK GDPR, the Data Protection Act 2018 and relevant employment legislation.

Acceptable Use Expectations

All users must:

- Use school systems primarily for professional and educational purposes.
- Act professionally and responsibly when using technology.
- Protect the reputation of the school.
- Respect copyright, intellectual property and licensing laws.
- Maintain appropriate professional boundaries.
- Follow safeguarding procedures at all times.

Users must not:

- Access, create, store or share illegal, harmful, extremist, discriminatory or inappropriate material.
- Deliberately bypass filtering, monitoring or security systems.
- Use school systems for personal business or commercial activity.
- Install unauthorised software or applications.
- Use another person's account or credentials.
- Engage in cyberbullying, harassment or discriminatory behaviour.
- Use technology in a way that could bring the school into disrepute.

Artificial Intelligence (AI) and Generative AI

Sele First recognises that generative AI tools may support teaching, administration and learning when used responsibly.

Examples include:

- Lesson planning support
- Administrative drafting
- Accessibility support
- Differentiation of learning materials
- Data analysis
- Educational research

However, AI tools also present safeguarding, accuracy, copyright, bias and data protection risks.

Staff Responsibilities When Using AI

Staff may only use AI tools that are approved or authorised by the school.

Staff must:

- Apply professional judgement to all AI-generated content.
- Fact-check and review outputs before use.
- Ensure AI-generated materials are age-appropriate and accurate.
- Avoid over-reliance on AI systems.
- Maintain transparency where significant AI assistance has been used.
- Ensure use aligns with safeguarding and equality duties.
- Follow copyright and intellectual property requirements.

Staff must not:

- Input confidential, personal or sensitive school data into public AI tools.
- Input pupil personal data into AI systems unless explicitly approved and compliant with UK GDPR.
- Use AI to generate safeguarding, SEND or behavioural judgments without professional oversight.
- Use AI to replace professional decision-making.
- Use AI to create inappropriate, discriminatory or misleading content.
- Use AI-generated images or audio in ways that could misrepresent individuals.

Any concerns relating to AI misuse, harmful content or data breaches must be reported immediately to the DSL, Headteacher or Data Protection Lead.

Devices, Equipment and Security

School Devices

School devices and systems are provided for professional use.

Staff must:

- Keep devices secure at all times.
- Lock devices when unattended.
- Use strong passwords and MFA.
- Report lost, stolen or damaged devices immediately.
- Ensure devices are updated regularly.
- Return equipment when requested.

Staff must not:

- Share login credentials.
- Leave devices unattended in insecure locations.
- Disable security software.
- Connect unauthorised devices to the school network.

Personal Devices

Use of personal devices on school premises must comply with this policy and any BYOD procedures.

Staff must:

- Keep personal devices secure.
- Store mobile phones appropriately during teaching time.
- Disable notifications where appropriate.
- Ensure smartwatches do not disrupt learning or compromise safeguarding.

Staff must not:

- Use personal devices to photograph, record or contact pupils.
- Use personal devices to store school confidential data unless authorised.
- Use personal devices in a manner that breaches professional conduct expectations.

School-issued equipment must be used for photography, video and communication relating to pupils.

Passwords and Authentication

Staff must:

- Use strong and unique passwords.

- Keep passwords confidential.
- Use multi-factor authentication where provided.
- Change passwords immediately if compromise is suspected.
- Log out of systems when finished.

Passwords must never be shared or written in insecure locations.

Internet and Online Use

Internet access is provided to support teaching, learning and school operations.

Staff must:

- Use the internet professionally and responsibly.
- Supervise pupils appropriately online.
- Report accidental access to inappropriate content.
- Ensure online resources are suitable and age-appropriate.
- Promote online safety within teaching.

Staff must not:

- Access inappropriate or illegal material.
- Download unauthorised software or files.
- Attempt to bypass filtering systems.
- Use anonymous proxies or VPNs without authorisation.

The school uses filtering and monitoring systems in line with DfE expectations.

Email and Communication

All staff are provided with a professional school email account.

Staff must:

- Use school email accounts for school business.
- Use MFA where required.
- Verify recipients before sending sensitive information.
- Report phishing or suspicious emails immediately.
- Use professional language and conduct.

Staff must not:

- Use personal email accounts for school business.
- Share confidential information insecurely.
- Open suspicious attachments or links.
- Send offensive, discriminatory or inappropriate content.

Communication with pupils and parents/carers must only occur through approved school systems and platforms.

Social Media and Professional Conduct

Staff must maintain professional standards online.

Staff should:

- Use appropriate privacy settings.
- Consider the long-term impact of online activity.
- Maintain clear professional boundaries.
- Ensure online conduct does not damage public trust.

Staff must not:

- Communicate privately with pupils using personal accounts.
- Share confidential school information online.
- Post content that could bring the school into disrepute.
- Identify the school in inappropriate online contexts.
- Engage in online behaviour that may undermine professional standards.

Any online safeguarding concerns must be reported immediately.

Photography, Video and Media

Sele First recognises that digital media can support learning and celebration of achievement.

Staff must:

- Use only authorised school equipment for recording pupils.
- Follow school consent procedures.
- Store images securely.
- Use images appropriately and professionally.

Staff must not:

- Use personal devices to photograph or record pupils.
- Share images without authorisation.
- Upload pupil images to personal or public platforms.

The school website and social media accounts will be monitored regularly to ensure content remains appropriate and compliant.

Data Protection and Information Security

All staff are responsible for protecting personal and confidential data.

Staff must comply with:

- UK GDPR
- Data Protection Act 2018

- School data protection procedures

Staff must:

- Access only information required for their role.
- Store data securely.
- Use encrypted storage where required.
- Dispose of confidential information securely.
- Report suspected data breaches immediately.

Staff must not:

- Share confidential information inappropriately.
- Transfer data using unauthorised systems.
- Store school data on personal cloud accounts.
- Remove sensitive data from school without authorisation.

Remote Working and Cloud Services

When working remotely, staff must:

- Use approved school platforms and systems.
- Ensure screens are not visible to unauthorised individuals.
- Maintain confidentiality.
- Use secure internet connections.
- Follow safeguarding expectations during online teaching.

Staff should avoid using public Wi-Fi unless using approved secure access methods.

Safeguarding and Online Safety

All staff have a responsibility to safeguard pupils online.

Staff must:

- Remain vigilant to online safety concerns.
- Report concerns immediately to the DSL.
- Follow safeguarding procedures.
- Teach and model safe online behaviours.
- Understand filtering and monitoring responsibilities.

Examples of concerns include:

- Exposure to harmful or extremist content
- Cyberbullying
- Online exploitation
- Inappropriate contact
- Self-harm or suicide-related content
- AI-generated harmful content

- Data breaches

Any safeguarding concern must be treated seriously and reported immediately.

Monitoring and Filtering

Sele First operates filtering and monitoring systems in accordance with DfE guidance.

Monitoring systems may identify:

- Safeguarding concerns
- Attempts to access inappropriate content
- Cybersecurity risks
- Policy breaches

Filtering and monitoring systems are reviewed regularly by school leaders and governors.

Training

All staff will receive appropriate training relating to:

- Safeguarding
- Online safety
- Cybersecurity
- Data protection
- Filtering and monitoring
- Artificial intelligence
- Professional conduct online

Training will be updated regularly in line with emerging technologies and DfE guidance.

Reporting Concerns

Staff must report immediately:

- Safeguarding concerns
- Suspected data breaches
- Lost or stolen devices
- Cybersecurity incidents
- Inappropriate content
- AI misuse
- Concerns regarding filtering or monitoring systems

Reports should be made to:

- Designated Safeguarding Lead (DSL)
- Headteacher
- Computing Lead
- Data Protection Lead

Sanctions

Failure to comply with this policy may result in:

- Removal of access rights
- Internal investigation
- Disciplinary action
- Referral to external agencies
- Referral to the Local Authority
- Referral to the police where appropriate

Serious breaches may constitute gross misconduct.

Relevant Legislation and Guidance

This policy reflects current legislation and guidance including:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Communications Act 2003
- Malicious Communications Act 1988
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Equality Act 2010
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Keeping Children Safe in Education (KCSIE) 2026
- DfE Filtering and Monitoring Standards
- DfE Meeting Digital and Technology Standards in Schools and Colleges
- DfE Generative Artificial Intelligence Guidance for Schools and Colleges
- UK Council for Internet Safety (UKCIS) guidance

Policy Review Cycle: Annual

Latest Review: July 2026

Next Scheduled Review: July 2027