

Feniscowles Primary School

Digital Technology, Online Safety and Acceptable Use Policy 2026/27

Striving for Excellence

Policy status	School policy
Applies to	All pupils, staff, governors, volunteers, visitors, contractors and other authorised users
Policy owner	Headteacher
Safeguarding lead	Designated Safeguarding Lead
Technical support	School’s contracted ICT support provider
Approval	Governing Body
Review frequency	At least annually and following significant changes or incidents
Academic year	2026/27

Document version history

Version	Date	Summary of changes	Author
v1.0	September 2026	New policy issued for 2026/27, aligned to Keeping Children Safe in Education 2026 and the DfE digital and AI Core Standards.	Headteacher

1. Policy statement

Feniscowles Primary School recognises that digital technology is an important part of children's education and of the effective operation of the school.

Technology provides significant opportunities for teaching, learning, communication, inclusion and creativity. It can also expose children and adults to safeguarding, privacy, security and wellbeing risks.

The school has a statutory responsibility to safeguard children online as well as offline.

Online safety is therefore not solely an ICT issue. It forms part of the school's whole-school safeguarding arrangements and should be considered alongside child protection, behaviour, curriculum, staff conduct, data protection and cyber security.

This policy establishes how Feniscowles Primary School will:

- provide a safe digital environment;
- educate pupils to use technology safely, responsibly and confidently;
- maintain appropriate filtering and monitoring arrangements;
- protect school systems, information and personal data;
- establish clear standards for acceptable use;
- manage emerging technologies, including generative artificial intelligence;
- respond appropriately to online safeguarding concerns and technology incidents;
- ensure staff understand their responsibilities;
- involve parents and carers in keeping children safe online.

Where an online or digital incident raises concerns about a child's safety or welfare, safeguarding procedures take precedence over generic ICT or disciplinary procedures.

2. Legislative and guidance framework

This policy has regard to current legislation and national guidance, including:

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children
- DfE Filtering and Monitoring Core Standard
- DfE Cyber Security Core Standard
- DfE Digital Leadership and Governance Core Standard
- DfE Meeting Digital and Technology Standards in Schools and Colleges
- DfE Generative Artificial Intelligence in Education guidance
- DfE Generative AI Product Safety Standards
- DfE Mobile Phones in Schools statutory guidance
- DfE Behaviour in Schools guidance
- DfE Teaching Online Safety in Schools guidance
- UKCIS guidance on sharing nudes and semi-nudes
- UK GDPR

- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Prevent Duty guidance
- Equality Act 2010
- Human Rights Act 1998
- relevant National Cyber Security Centre guidance.

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy;
- Behaviour Policy;
- Staff Code of Conduct;
- Data Protection Policy;
- AI Policy and associated AI governance arrangements;
- Prevent procedures;
- mobile phone expectations;
- curriculum policies;
- complaints procedures;
- disciplinary procedures.

Where legislation or statutory safeguarding guidance changes during the lifetime of this policy, the school will apply the current requirements.

3. Scope

This policy applies to all use of digital technology connected with Feniscowles Primary School.

It applies to:

- school-owned devices;
- local authority devices and systems;
- school networks and internet connections;
- computers, laptops and tablets;
- mobile phones and smart devices;
- cameras and recording devices;
- cloud services;
- school email;
- management information systems;
- safeguarding systems;
- communication and learning platforms;
- filtering and monitoring systems;
- artificial intelligence systems;

- social media where its use relates to the school;
- remotely accessed school systems;
- personal devices used for school business;
- removable storage devices;
- any digital system processing school or pupil information.

The requirements apply whether technology is being accessed:

- on the school premises;
- away from school;
- during educational visits;
- while working from home;
- through a school-owned device;
- through an authorised personal device.

4. Principles of online safety

Feniscowles Primary School approaches online safety as part of safeguarding.

The school's approach is informed by the four broad areas of online risk.

4.1 Content

Children may encounter harmful or inappropriate material, including:

- pornography;
- sexualised material;
- violence;
- racism;
- misogyny;
- hate material;
- extremist material;
- material promoting self-harm or suicide;
- harmful challenges;
- misinformation and disinformation;
- content promoting eating disorders;
- inappropriate AI-generated material.

4.2 Contact

Children may experience harmful interaction with other people, including:

- grooming;
- sexual exploitation;
- coercion;
- bullying;

- harassment;
- contact from strangers;
- exploitation by criminal groups;
- radicalisation;
- inappropriate contact through games, social media or messaging services.

4.3 Conduct

Children's own online behaviour may create risks, including:

- cyberbullying;
- harmful communication;
- sexual harassment;
- sharing personal information;
- creating or sharing sexual imagery;
- impersonation;
- misuse of images;
- inappropriate use of AI;
- deliberate attempts to bypass school safeguards.

4.4 Commerce

Children may encounter commercial and financial risks, including:

- scams;
- fraud;
- gambling;
- inappropriate advertising;
- in-game spending;
- financial exploitation;
- phishing;
- misleading commercial content.

The school recognises that new technologies may change the way these risks appear. Its safeguards will therefore be reviewed regularly rather than being limited to named applications or websites.

5. Roles and responsibilities

5.1 Governing Body

The Governing Body has strategic responsibility for ensuring appropriate arrangements are in place to safeguard children using technology.

Governors will:

- ensure the school has appropriate filtering and monitoring systems;

- receive assurance that filtering and monitoring arrangements are reviewed at least annually;
- identify a governor to provide appropriate oversight of filtering and monitoring;
- ensure appropriate cyber security arrangements are maintained;
- provide oversight of digital technology strategy and risk;
- ensure appropriate policies and procedures are in place;
- ensure significant online safeguarding and cyber risks are considered through the school's governance arrangements;
- ensure staff receive appropriate training.

Governors are not expected to undertake technical management of school systems.

5.2 Headteacher

The Headteacher has overall executive responsibility for implementation of this policy.

The Headteacher will ensure that:

- appropriate safeguarding and technical systems are in place;
- staff understand their responsibilities;
- filtering and monitoring arrangements are reviewed;
- digital and cyber risks are appropriately assessed;
- approved systems are used for school business;
- appropriate data protection safeguards are applied;
- significant breaches or incidents are escalated appropriately;
- governors receive sufficient information to provide assurance;
- suitable technical support arrangements are maintained.

5.3 Designated Safeguarding Lead

The DSL takes lead responsibility for safeguarding and child protection, including online safety.

The DSL will:

- understand the school's filtering and monitoring arrangements;
- understand their capabilities and limitations;
- receive or have appropriate access to relevant monitoring information;
- ensure safeguarding alerts are assessed promptly;
- determine when online activity represents a safeguarding concern;
- ensure relevant concerns are recorded in accordance with the school's safeguarding procedures;
- coordinate safeguarding responses;
- make referrals to external agencies where necessary;
- contribute to the annual filtering and monitoring review;
- identify changing patterns of online harm;
- ensure safeguarding learning informs staff training and pupil education.

Deputy DSLs will fulfil these functions when acting on behalf of the DSL.

5.4 Digital/ICT leadership

The school's digital leadership arrangements will support:

- effective use of educational technology;
- curriculum implementation;
- implementation of approved digital systems;
- staff competence;
- appropriate procurement;
- online safety education;
- liaison between safeguarding, curriculum and technical functions.

Technical responsibility must not be confused with safeguarding responsibility.

5.5 ICT technical support provider

The school's technical support provider will work under the authority of the Headteacher and will:

- maintain agreed technical security measures;
- maintain supported operating systems and software;
- implement security updates;
- support filtering and monitoring systems;
- maintain appropriate security logs;
- maintain backup arrangements;
- support account management;
- support implementation of multi-factor authentication;
- support investigation of cyber incidents;
- preserve technical evidence where required;
- assist with business continuity and recovery;
- notify the school promptly of significant security concerns;
- support the annual review of filtering and monitoring;
- provide information necessary for governors and leaders to understand the effectiveness and limitations of systems.

The school's current contracted ICT provider is Crystal AV IT Ltd unless contractual arrangements change.

The school's filtering and monitoring system is Smoothwall, unless replaced by an alternative system approved by the Headteacher and Governing Body.

5.6 Data Protection Officer

The DPO provides independent advice and oversight regarding data protection.

The DPO should be involved where appropriate in:

- significant personal data breaches;

- Data Protection Impact Assessments;
- introduction of higher-risk digital systems;
- use of artificial intelligence involving personal data;
- contractual arrangements involving personal information.

5.7 All staff

All staff have a responsibility for online safety.

Staff must:

- follow this policy and the Staff Code of Conduct;
- maintain professional boundaries;
- actively supervise pupils' use of technology;
- report safeguarding concerns immediately;
- report technical security concerns;
- protect passwords and accounts;
- use approved systems;
- protect personal information;
- follow school requirements relating to AI;
- challenge and report inappropriate technology use;
- support pupils to become safe and responsible digital citizens.

Filtering and monitoring technology does not replace effective adult supervision.

6. Filtering

The school will operate appropriate filtering to reduce the risk of access to illegal, harmful or inappropriate material.

Filtering will be appropriate to:

- the age of pupils;
- the school's curriculum;
- the needs of pupils;
- identified safeguarding risks;
- the technology being used.

The school recognises that no filtering solution is capable of eliminating all online risk.

Filtering should protect pupils without unnecessarily restricting legitimate teaching and learning or preventing pupils from developing their ability to understand and manage online risks.

The school will understand:

- what its filtering system covers;
- which devices are protected;
- whether filtering continues when devices are used away from school;

- which users and accounts are covered;
- categories of material that are blocked;
- how exceptions are managed;
- how concerns are reported;
- the limitations of the system.

Staff and pupils must not attempt to disable, bypass or interfere with filtering arrangements.

Attempts by pupils to circumvent filtering will be considered both as a behaviour matter and, where appropriate, a potential safeguarding indicator.

Attempts by adults to circumvent safeguards may constitute misconduct.

7. Monitoring

Monitoring is used to identify potentially harmful or inappropriate activity.

It may include:

- automated technical monitoring;
- reports and alerts;
- review of network activity;
- review of school-owned devices;
- staff observation of pupil screens;
- classroom supervision.

Monitoring arrangements will be proportionate to the school's context and risk profile.

The school will have arrangements for:

- routine review of monitoring information;
- weekly monitoring information or reporting where provided by the school's technical solution;
- immediate escalation of high-risk safeguarding alerts;
- prompt consideration of concerning searches or activity;
- recording action taken;
- identifying repeated patterns;
- escalating safeguarding concerns to the DSL.

High-risk alerts should not wait for a routine report.

Staff must continue to monitor pupil use directly when children are using technology. Staff should position themselves so that they can reasonably observe pupil activity and intervene where necessary.

8. Filtering and monitoring review

The school will conduct a formal review of filtering and monitoring arrangements at least annually.

The review will involve:

- a member or members of SLT;
- the DSL;
- ICT technical support;
- the responsible governor.

The review will be recorded.

It will consider:

- current filtering provision;
- monitoring arrangements;
- identified gaps;
- safeguarding incidents;
- pupil and staff needs;
- age and developmental stage;
- SEND;
- communication needs;
- EAL;
- known safeguarding vulnerabilities;
- local safeguarding risks;
- devices used in school;
- devices used remotely;
- new online services;
- artificial intelligence;
- the ability of systems to respond to real-time, dynamic and personalised content.

Reviews will also take place following:

- a significant safeguarding incident;
- a significant cyber security incident;
- material changes to the network;
- introduction of major new technology;
- identification of a significant weakness.

9. Filtering and monitoring assurance checks

In addition to the formal annual review, proportionate checks will be undertaken to assure leaders that arrangements remain effective.

Checks should, over time, cover relevant:

- school sites;
- networks;
- pupil devices;
- staff devices;

- pupil accounts;
- staff accounts;
- guest access;
- browsers;
- search engines;
- off-site use of managed devices where applicable.

Records should identify:

- the date;
- who conducted the check;
- what was tested;
- the outcome;
- any required action;
- confirmation that action has been completed.

Given the school's physical organisation, checks must provide reasonable assurance that safeguarding controls operate effectively across both school sites.

10. Pupil accounts and passwords

Individual accounts should be used wherever technically practicable.

Pupils will normally have individual credentials appropriate to their age and developmental stage.

Shared or generic pupil accounts should only be used where there is a clear operational or technical reason and where this has been considered by school leadership and ICT support.

Wherever reasonably possible, activity should be attributable to an individual user or device.

Pupils must:

- keep passwords private;
- not use another person's account;
- report suspected compromise;
- log out when appropriate;
- treat other people's files and accounts respectfully.

Account security will be taught in an age-appropriate way.

11. Staff accounts and authentication

Staff must use their own accounts.

Staff must not:

- share credentials;
- use another member of staff's account;
- allow pupils to use staff accounts;

- leave authenticated devices unsecured.

Passwords should:

- be sufficiently long;
- be unique;
- not be reused across unrelated services;
- not be based on easily obtainable personal information.

Routine password changes will not be required solely because a fixed period has elapsed unless required by a particular system or security standard.

Passwords must be changed promptly where compromise is known or suspected.

Multi-factor authentication will be enabled for appropriate systems wherever technically available and required by the school's security arrangements.

Staff should use approved password-management arrangements where these are provided by the school.

12. Acceptable use by staff

School technology is primarily provided for professional and educational purposes.

Reasonable incidental personal use may be permitted where it:

- does not interfere with professional duties;
- does not occur during teaching where it detracts from pupils;
- does not create security risk;
- does not result in additional material cost;
- does not bring the school into disrepute;
- complies with this policy.

Staff must not use school technology to:

- access illegal material;
- access pornography except where specifically authorised as part of legitimate safeguarding or technical duties;
- bully, harass or intimidate;
- discriminate;
- access or promote extremist material for inappropriate purposes;
- engage in gambling;
- conduct personal commercial activity;
- infringe copyright deliberately;
- gain unauthorised access to systems;
- disable security measures;
- create malicious software;
- deliberately distribute malware;
- impersonate another person;

- create harmful or deceptive deepfakes;
- create, access or distribute sexualised imagery unlawfully;
- use technology in a manner incompatible with professional conduct.

Any accidental access to illegal or seriously inappropriate material must be reported immediately. Staff should not deliberately continue viewing the material.

Added cross-reference: Any allegation of misconduct by a member of staff involving online conduct will additionally be managed in accordance with the school's Allegations Against Staff / LADO (Local Authority Designated Officer) procedures, in line with Part 4 of Keeping Children Safe in Education, alongside the school's generic disciplinary procedures referenced above.

13. Professional communication

Staff must maintain professional boundaries when communicating electronically.

Staff will use school-approved communication systems for communication with pupils and parents.

Staff must not normally:

- use personal social media accounts to communicate privately with pupils;
- add or follow current pupils through personal social media accounts;
- use personal messaging accounts for routine pupil communication;
- disclose confidential school information through personal communication systems.

Electronic communications should be:

- professional;
- respectful;
- necessary;
- appropriate;
- capable of proper accountability.

School communications may be subject to disclosure where required by law.

14. Social media

Staff are entitled to a private life but must maintain professional standards.

Staff must not publish information that:

- breaches pupil or staff confidentiality;
- identifies safeguarding information;
- brings pupils into inappropriate public discussion;
- constitutes bullying, harassment or discrimination;
- undermines professional boundaries;
- creates a safeguarding risk.

Images of pupils must only be published through authorised school systems and in accordance with school consent and safeguarding arrangements.

Staff should use appropriate privacy controls but must understand that online content can be copied, shared and redistributed beyond its intended audience.

15. Pupil acceptable use

Pupils will be taught to use school technology responsibly.

Age-appropriate acceptable use agreements will be used for pupils.

Pupils are expected to:

- use technology for appropriate purposes;
- follow staff instructions;
- use their own account where provided;
- keep passwords private;
- protect personal information;
- communicate respectfully;
- tell an adult if something online worries or upsets them;
- report inappropriate material;
- respect other people's work;
- respect copyright;
- use approved services;
- treat equipment carefully.

Pupils must not deliberately:

- bypass filtering;
- access another person's account;
- access harmful or inappropriate material;
- bully or harass others;
- share another person's private information;
- create or share harmful images;
- access inappropriate games or services;
- interfere with networks or devices;
- download unauthorised software;
- use AI in ways prohibited by staff or school policy.

Responses to misuse will take account of:

- age;
- understanding;
- intent;
- SEND;
- vulnerability;

- repetition;
- safeguarding context.

Safeguarding concerns will not be treated merely as misconduct.

16. Generative artificial intelligence

The school recognises that generative AI can support teaching, learning and school administration when used appropriately.

AI also creates risks relating to:

- safeguarding;
- inaccurate information;
- bias;
- privacy;
- data protection;
- intellectual property;
- manipulation;
- inappropriate content;
- academic integrity;
- impersonation;
- deepfakes;
- over-reliance.

AI tools used for school purposes must be consistent with the school's AI governance arrangements.

Staff use

Staff must:

- use approved AI systems for school work;
- comply with data-protection requirements;
- check AI-generated information before using it;
- take professional responsibility for final outputs;
- consider copyright and intellectual-property implications;
- ensure AI use does not undermine assessment integrity;
- consider safeguarding implications before showing AI-generated material to pupils.

Staff must not enter identifiable or confidential pupil information into an AI system unless that specific processing has been approved and appropriately assessed.

AI output must not be assumed to be accurate because it has been generated confidently.

Pupil use

Pupils may only use generative AI:

- for an authorised educational purpose;

- using an approved service;
- where any applicable age requirements are satisfied;
- under appropriate adult direction or supervision;
- in accordance with the school's curriculum and assessment expectations.

The school will consider the safeguarding capabilities of AI products before introducing them for pupil use.

Prohibited AI use

Users must not use AI to:

- create harmful or sexual content;
- generate or manipulate nude or semi-nude imagery;
- bully or humiliate another person;
- impersonate pupils, staff or parents;
- fabricate harmful communications;
- create malicious deepfakes;
- process confidential information without authority;
- circumvent safeguarding restrictions;
- deliberately deceive where authenticity is required.

AI-generated harmful content will be treated according to its nature and impact rather than being regarded as less serious simply because it was artificially generated.

17. Mobile phones and smart devices

The school will maintain an environment in which pupils do not use mobile phones during the school day in accordance with statutory national guidance.

This includes:

- lessons;
- transitions;
- breaktimes;
- lunchtimes;
- assemblies;
- school-organised activities during the school day.

Where pupils are permitted to bring a phone to school, it must be stored in accordance with school procedures and not used during the school day.

The school may make proportionate exceptions where required for:

- medical reasons;
- disability or SEND;
- safeguarding;
- another exceptional need authorised by the Headteacher.

Smart watches and other connected personal devices may be subject to equivalent restrictions where their functionality creates the same risks.

Detailed consequences and confiscation arrangements are set out through the school's Behaviour Policy and associated procedures.

18. Personal devices and BYOD

Staff should use school-managed equipment for school business wherever reasonably practicable.

Where use of a personal device is permitted:

- the device must have appropriate security;
- a passcode or biometric authentication must be enabled;
- the operating system must be supported and updated;
- personal data must not be stored unnecessarily;
- school information should be accessed through approved systems;
- confidential school information must not be retained in personal applications;
- the device must not be shared with others while school information is accessible.

The school may withdraw access where a device presents an unacceptable security risk.

19. Photography, video and audio

School equipment or authorised systems should normally be used to capture pupil images.

Staff must not routinely use personal phones or personal devices to photograph or record pupils.

Any exceptional circumstance must be authorised and managed in accordance with safeguarding and data-protection requirements.

Images must:

- have a legitimate school purpose;
- be stored securely;
- only be shared through approved systems;
- be deleted when no longer required in accordance with retention arrangements.

Staff must consider additional safeguarding implications where publication of an image could increase risk to a child.

20. Nudes, semi-nudes and sexually explicit imagery

Any incident involving nude or semi-nude images of children must be referred immediately to the DSL.

Staff must not investigate such incidents by unnecessarily viewing, copying, downloading, printing, forwarding or taking screenshots of the image.

Staff should not ask a child to send or show the image to them.

The DSL will follow current safeguarding and UKCIS guidance and determine whether referral to children's social care, police or another agency is required.

This approach applies whether imagery is:

- created by a child;
- created by another person;
- altered;
- digitally manipulated;
- generated using artificial intelligence.

AI-generated sexual imagery involving an identifiable child may create significant safeguarding harm even where no original photograph exists.

21. Online bullying, harassment and harmful conduct

Online behaviour will be addressed consistently with the school's Behaviour and Safeguarding policies.

The school will consider:

- the impact on the victim;
- whether behaviour is repeated;
- power imbalance;
- sexual harassment;
- prejudice-related behaviour;
- threats;
- coercion;
- exploitation;
- impersonation;
- distribution beyond the original audience.

Where online behaviour indicates that a child may be at risk of significant harm, the DSL will lead the response.

22. Extremism and radicalisation

The school's filtering and monitoring arrangements will support its responsibilities under the Prevent Duty.

Concerns about extremist material or possible radicalisation must be referred to the DSL.

The school recognises that legitimate curriculum study of controversial issues must not be unnecessarily prevented by filtering.

Staff requiring access to material that is blocked for legitimate educational purposes must follow the school's authorised process.

23. Online safety curriculum

Online safety will be taught progressively and revisited regularly.

Teaching will include age-appropriate learning about:

- privacy;
- personal information;
- passwords;
- respectful communication;
- cyberbullying;
- inappropriate contact;
- grooming;
- consent;
- images;
- misinformation;
- disinformation;
- scams;
- commercial influence;
- gaming;
- healthy technology habits;
- reporting concerns;
- copyright;
- AI literacy;
- appropriate use of generative AI.

Online safety will be reinforced through Computing, PSHE/RSHE and the wider safeguarding curriculum.

The curriculum will aim to develop children's ability to assess and manage online risk rather than relying entirely on technical restriction.

24. SEND and vulnerable pupils

The school recognises that online risk is not experienced equally by all children.

Filtering, monitoring, teaching and safeguarding arrangements will consider:

- SEND;
- communication difficulties;
- cognitive development;
- social understanding;
- emotional regulation;
- EAL;
- prior safeguarding concerns;

- contextual safeguarding factors;
- previous exploitation or abuse.

Reasonable adjustments may be made to enable safe access to technology.

Reasonable adjustments must not remove necessary safeguarding protections.

Staff should consider whether repeated or unusual online behaviour may communicate an unmet need or safeguarding concern.

25. Parent and carer partnership

Parents and carers play an important role in children's online safety.

The school will provide appropriate information about:

- online safety expectations;
- school filtering and monitoring;
- pupil acceptable use;
- mobile phones;
- emerging online risks;
- reporting concerns;
- sources of support.

Parents should report significant online incidents affecting pupils to the school where these may affect the child's wellbeing, safety or school life.

26. Cyber security

The school will maintain appropriate cyber security arrangements.

These will include, according to the systems in use:

- supported operating systems;
- security updates;
- endpoint protection;
- firewall protection;
- secure configuration;
- appropriate account permissions;
- multi-factor authentication;
- backup;
- recovery arrangements;
- network security;
- vulnerability management;
- staff awareness;
- incident response.

Access to systems will be granted on the basis of legitimate role requirements.

Administrative accounts will be restricted and should not be used for routine activity where separate accounts can reasonably be provided.

Leavers' access will be removed promptly.

Access rights will be reviewed periodically.

27. Phishing and malicious communications

Staff must remain alert to phishing and social-engineering attacks.

Suspicious messages should be reported through the school's agreed process.

Staff should not:

- open unexpected attachments;
- follow suspicious links;
- disclose credentials in response to an unsolicited request;
- approve unexpected MFA prompts;
- install software requested through suspicious communications.

Suspected compromise must be reported immediately.

28. Malware and unauthorised software

Users must not deliberately:

- introduce malware;
- disable security software;
- install unauthorised software;
- alter technical security settings;
- conduct unauthorised penetration testing;
- probe the network;
- attempt to gain unauthorised access.

Software must be properly licensed and installed through approved processes.

29. Data protection

Personal information must be processed lawfully, fairly and securely.

Users must:

- access only information required for their role;
- use approved systems;
- minimise unnecessary duplication;
- keep confidential information secure;
- avoid sending sensitive information through insecure channels;
- report data breaches immediately;

- comply with retention arrangements.

The school will use Data Protection Impact Assessments where processing is likely to create a high risk to individuals' rights and freedoms.

This may include certain:

- AI systems;
- monitoring systems;
- biometric systems;
- large-scale data-processing systems;
- new technologies involving sensitive information.

30. Cloud services

Only appropriately approved cloud services should be used for school information.

Before significant systems are introduced, the school will consider:

- data location;
- security;
- access control;
- contractual terms;
- data retention;
- supplier assurances;
- backup;
- deletion;
- privacy;
- safeguarding;
- business continuity.

Staff must not use personal cloud-storage accounts for confidential school information.

31. Removable media

Use of removable storage will be minimised.

Where removable media is authorised:

- school requirements must be followed;
- encryption must be used where required;
- confidential data must be protected;
- devices must be scanned appropriately;
- loss must be reported immediately.

Personally owned removable media should not be used for confidential school information unless specifically authorised.

32. Remote working

Staff accessing school systems remotely must:

- use secure devices;
- prevent unauthorised viewing;
- protect credentials;
- use approved systems;
- keep equipment physically secure;
- avoid leaving confidential information accessible to family members or others;
- ensure devices are locked when unattended.

Public or insecure networks should not be used for sensitive school activity unless an approved secure solution is available.

33. Physical security of equipment

Users must take reasonable care of school equipment.

Devices containing school information should:

- be securely stored;
- not be left visibly unattended in vehicles;
- be protected against theft;
- be locked when unattended;
- be returned when requested.

Loss or theft must be reported immediately.

Where a device contains personal data, the school's data-breach procedure must also be followed.

34. Asset management

The school will maintain an appropriate inventory of significant ICT equipment.

School devices taken away from the premises will remain the responsibility of the authorised user.

Users must return equipment:

- when requested;
- when employment ends;
- when it requires maintenance;
- when it is replaced.

Equipment will be disposed of securely, including secure destruction or removal of data.

35. Backup and business continuity

Critical school information will be backed up in accordance with agreed technical arrangements.

Backup arrangements will:

- protect against accidental loss;
- support recovery from cyber incidents;
- be appropriately secured;
- be tested periodically.

The school will maintain proportionate arrangements to continue essential:

- safeguarding;
- communication;
- administrative;
- teaching

functions during significant ICT disruption.

36. Reporting concerns

Safeguarding concerns

Any concern that a child may be at risk of harm must be reported immediately to the DSL or deputy DSL in accordance with the Safeguarding and Child Protection Policy.

Examples include:

- grooming;
- sexual exploitation;
- nude or semi-nude imagery;
- online sexual harassment;
- threats;
- self-harm or suicide material;
- radicalisation;
- significant bullying;
- exploitation;
- harmful AI-generated content involving a child.

Cyber security concerns

Cyber security incidents must be reported immediately to the appropriate school leader and ICT support provider.

Examples include:

- suspected compromised account;
- malware;
- ransomware;
- unauthorised access;
- unusual network activity;

- loss of a device;
- security-control failure.

Personal data breaches

Actual or suspected personal data breaches must be reported immediately through the school's data-breach procedure.

An incident may fall into more than one category.

Reporting a matter to ICT support does not replace a safeguarding referral to the DSL.

37. Responding to online safeguarding incidents

The DSL will determine the safeguarding response.

This may include:

- speaking to the child;
- securing immediate safety;
- preserving appropriate evidence;
- contacting parents where appropriate;
- consulting children's social care;
- contacting police;
- using local safeguarding procedures;
- making a Prevent referral;
- requesting technical information;
- providing pastoral support.

Staff should not conduct independent digital investigations where doing so could:

- increase risk;
- expose them to illegal imagery;
- compromise evidence;
- interfere with an external investigation.

38. Cyber incident response

Where a significant cyber incident occurs, the school will take proportionate action to:

1. identify the issue;
2. contain the threat;
3. protect children and information;
4. preserve appropriate evidence;
5. involve technical support;
6. notify relevant parties;
7. restore systems safely;

8. consider data-protection reporting requirements;

9. record decisions;

10. review lessons learned.

Where criminal activity is suspected, appropriate external agencies may be contacted.

39. Monitoring of staff and pupil systems

Users should understand that use of school systems may be logged and monitored for legitimate purposes including:

- safeguarding;
- cyber security;
- system management;
- investigation of misuse;
- legal compliance;
- maintaining availability and integrity.

Monitoring will be proportionate and undertaken in accordance with relevant legal requirements.

Users should have no expectation that activity conducted through school systems is entirely private.

This does not give the school unrestricted authority to monitor personal activity unrelated to legitimate school purposes.

40. Searching and confiscation

Where a school-owned or personal device is searched or confiscated, staff will follow current statutory guidance and the school's Behaviour and Safeguarding policies.

Staff must not independently delete suspected safeguarding evidence.

Where illegal material or sexual imagery involving children may be present, the DSL must be involved and appropriate national guidance followed.

41. Copyright and intellectual property

Users must respect intellectual-property rights.

Software must be properly licensed.

Staff and pupils should not deliberately:

- reproduce copyrighted material unlawfully;
- install pirated software;
- distribute protected content without permission.

Use of AI does not remove copyright responsibilities.

Where staff use externally created resources, they should comply with applicable licensing conditions.

42. Visitors, volunteers and temporary users

Temporary users will be given access only where required.

Access should:

- reflect the person's role;
- be limited in duration;
- provide only necessary permissions;
- be removed when no longer required.

Visitors, contractors and volunteers using school technology must comply with relevant elements of this policy.

Those with privileged technical access are subject to enhanced confidentiality and security expectations.

43. Technical administrators and privileged accounts

Individuals with elevated technical access must:

- use access only for authorised purposes;
- maintain confidentiality;
- avoid routine use of privileged accounts where separate standard accounts are available;
- ensure significant administrative actions are capable of audit;
- follow change-control arrangements;
- report security concerns immediately.

Access to another person's files should only occur where there is a legitimate and authorised reason.

44. Unacceptable use

The following are examples of unacceptable use:

- unauthorised access to another person's account;
- password sharing;
- deliberate bypassing of filters;
- hacking;
- testing security without authority;
- installation of unauthorised software;
- malware creation or distribution;
- cyberbullying;
- harassment;

- discrimination;
- accessing illegal material;
- creation or sharing of harmful sexual material;
- malicious impersonation;
- harmful deepfakes;
- unauthorised disclosure of confidential information;
- deliberate damage to school equipment;
- unauthorised commercial use;
- unlawful copyright infringement;
- deliberate creation or distribution of harmful misinformation;
- inappropriate AI use;
- any use that creates a significant safeguarding, professional or security risk.

This list is not exhaustive.

45. Consequences of misuse

The school will respond proportionately to misuse.

For pupils this may involve:

- education and restorative work;
- increased supervision;
- restriction of technology access;
- consequences under the Behaviour Policy;
- parental involvement;
- safeguarding intervention;
- referral to external agencies.

For staff, breaches may result in:

- management action;
- restriction of systems access;
- investigation;
- disciplinary procedures;
- safeguarding referral;
- referral to external agencies where appropriate.

The response will depend on the nature, intent, impact and context of the incident.

46. Training

All staff will receive appropriate information and training relating to:

- online safety;
- filtering and monitoring;

- safeguarding reporting;
- cyber security;
- phishing;
- password security;
- data protection;
- safe use of AI;
- emerging risks.

The DSL and relevant leaders will maintain appropriate knowledge of filtering and monitoring. Governors will receive sufficient information and training to exercise appropriate oversight.

47. Acceptable Use Agreements

The school will maintain separate, accessible Acceptable Use Agreements appropriate to different users.

These will normally include:

- Staff Acceptable Use Agreement
- KS1/EYFS age-appropriate online safety expectations
- KS2 Pupil Acceptable Use Agreement
- parent/carers acknowledgement where appropriate
- temporary user or contractor arrangements where required.

The agreements will summarise the practical expectations established by this policy.

48. Policy review

This policy will be reviewed at least annually.

Earlier review will take place where necessary following:

- changes to statutory guidance;
- changes to DfE digital standards;
- significant safeguarding incidents;
- cyber security incidents;
- introduction of significant new technologies;
- significant changes to school systems;
- changes to legislation;
- identified weaknesses in current arrangements.

The annual review should consider evidence from:

- safeguarding records;
- filtering and monitoring;
- cyber incidents;
- technical checks;

- pupil experience;
- staff experience;
- curriculum monitoring;
- relevant local and national developments.

Appendix 1: Staff Acceptable Use Agreement

I understand that the school's technology systems are provided primarily to support education and school business.

I will:

- use school technology professionally and responsibly;
- maintain confidentiality;
- protect my account and password;
- use approved systems for school information;
- lock devices when unattended;
- report suspected compromise promptly;
- maintain professional communication with pupils and parents;
- actively supervise pupils when they use technology;
- report online safeguarding concerns immediately to the DSL;
- report cyber security concerns promptly;
- report personal data breaches immediately;
- comply with filtering and monitoring arrangements;
- respect copyright;
- follow the school's AI Policy and approved AI arrangements;
- check AI-generated information before using it professionally;
- take responsibility for material I create or distribute;
- protect school devices issued to me.

I will not:

- share my password;
- allow pupils to access a staff account;
- deliberately bypass filtering or security systems;
- use personal email for confidential school information;
- store confidential school information in unauthorised personal cloud services;
- photograph pupils using my personal device except where specifically authorised;
- communicate privately with pupils through personal social media;
- upload identifiable or confidential pupil information into an unauthorised AI service;
- use AI to create harmful, deceptive or inappropriate content;
- deliberately access illegal or seriously inappropriate material;
- conduct unauthorised security testing;
- install unauthorised software.

I understand that use of school systems may be logged and monitored for legitimate safeguarding, security, administrative and legal purposes.

I understand that safeguarding concerns take precedence over generic ICT procedures.

Name: _____

Signature: _____

Date: _____

Appendix 2: KS2 Pupil Acceptable Use Agreement

My technology agreement

When I use technology at Feniscowles Primary School:

I will:

- use technology for the activity my teacher has asked me to do;
- keep my password private;
- use my own account;
- be kind and respectful;
- look after school equipment;
- tell an adult if something online worries, frightens or upsets me;
- tell an adult if I see something inappropriate;
- ask before sharing information about myself;
- respect other people's work;
- use AI only when my teacher says I can;
- tell a member of staff if I make a mistake online.

I will not:

- try to get around the school's internet filters;
- use another person's account;
- search for harmful or inappropriate material;
- send unkind or threatening messages;
- take or share pictures of people without permission;
- share private information;
- install games or software without permission;
- use AI to pretend to be someone else or create harmful content.

If something goes wrong online, I know I can tell an adult in school.

Telling an adult about something that has worried me is the right thing to do.

Pupil: _____

Date: _____

Appendix 3: EYFS and KS1 Online Safety Agreement

I stay safe when I use technology

I will:

- use the device carefully;
- listen to my grown-up;
- use kind words;
- keep my password private;
- tell a grown-up if I see something that worries me;
- ask before I click something I do not understand;
- stop and tell an adult if something does not feel right.

Stop. Close. Tell.

If I see something that worries me:

STOP using it.

CLOSE or turn away from it.

TELL a trusted adult.

Appendix 4: Online Safety and Digital Incident Reporting Routes

Safeguarding

If an incident may involve harm or risk of harm to a child:

Report immediately to the DSL or Deputy DSL.

This includes:

- grooming;
- sexual imagery;
- exploitation;
- cyberbullying creating safeguarding concerns;
- self-harm or suicide content;
- radicalisation;
- harmful sexual behaviour;
- serious online threats;
- AI-generated harmful imagery.

Record the concern through the school's safeguarding system as directed.

Cyber security

If an incident involves:

- malware;
- hacked accounts;
- ransomware;
- suspicious network activity;
- security failure;
- unauthorised system access;

inform the appropriate school leader and ICT technical support immediately.

Personal data

If personal information:

- is sent to the wrong person;
- is lost;
- is stolen;
- is accessed without authority;
- is disclosed accidentally;

follow the school's personal data breach procedure immediately.

Remember

One incident can require more than one response.

A cyber incident can also be a safeguarding incident.

A safeguarding concern must not be left solely with ICT support.

Appendix 5: Filtering and Monitoring Annual Review Record

The annual review should record:

Date of review: _____

SLT representative: _____

DSL: _____

ICT support representative: _____

Responsible governor: _____

The review should consider

- ☐ Current filtering system
- ☐ Current monitoring system
- ☐ Devices covered
- ☐ On-site coverage
- ☐ Off-site coverage
- ☐ Staff accounts
- ☐ Pupil accounts
- ☐ Guest access
- ☐ Both school sites
- ☐ Safeguarding alerts
- ☐ Weekly monitoring information
- ☐ SEND and vulnerable pupils
- ☐ Age and developmental needs
- ☐ EAL
- ☐ AI-generated and dynamic content
- ☐ New apps and services
- ☐ Attempts to bypass filtering
- ☐ Curriculum impact
- ☐ Significant incidents
- ☐ Technical limitations

Identified strengths

Identified gaps or risks

Required actions

Action owner: _____

Completion date: _____

Reported to governors: _____

Appendix 6: Filtering and Monitoring Check Record

Date: _____

Person completing check: _____

Site: _____

Device/account tested: _____

What was tested: _____

Outcome: _____

Issue identified: _____

Action required: _____

Person responsible: _____

Completion confirmed: _____

Policy approval

Approved by Governing Body: _____

Date: _____

Chair of Governors: _____

Headteacher: _____

Next formal review: September 2027, or earlier if required.

Appendix 7: Definitions and abbreviations

For ease of reference, the following abbreviations used throughout this policy are set out below.

Term	Meaning
DSL	Designated Safeguarding Lead
DPO	Data Protection Officer
KCSIE	Keeping Children Safe in Education (statutory DfE guidance)
UKCIS	UK Council for Internet Safety
SEND	Special Educational Needs and Disabilities
EAL	English as an Additional Language
GDPR	General Data Protection Regulation (as it forms part of UK law — ‘UK GDPR’)
MFA	Multi-Factor Authentication
BYOD	Bring Your Own Device
AI	Artificial Intelligence, including generative AI systems
LADO	Local Authority Designated Officer, responsible for managing allegations against staff and volunteers
PSHE/RSHE	Personal, Social, Health and Economic education / Relationships, Sex and Health Education
ICT	Information and Communications Technology
SLT	Senior Leadership Team