

Barn Croft Primary School

Online Safety Policy



Version no.	Date	Approved by	Review Frequency	Review Date
2	September 2026	Governing Body	+1 Years	September 2027

Aims

Barn Croft Primary School recognises that technology is an important part of children's learning, communication and everyday lives. We want pupils to benefit from technology while developing the knowledge, skills and confidence to use it safely and responsibly.

- protect pupils, staff and the wider school community from online harm;
- teach pupils how to recognise, assess and manage online risks;
- support pupils to behave respectfully and responsibly online;
- provide clear processes for reporting and responding to online safety concerns;
- ensure that filtering and monitoring arrangements support safeguarding and learning;
- identify pupils who may be particularly vulnerable to online harm and provide appropriate support;
- work in partnership with parents and carers to promote safe use of technology at home and at school.

Online risks are considered under the four broad areas of content, contact, conduct and commerce.

Legislation and guidance

This policy is informed by the following current guidance and legislation, including:

- Keeping Children Safe in Education 2026 (KCSIE);
- Education Act 1996 and Education and Inspections Act 2006;
- Equality Act 2010;
- Data Protection Act 2018 and UK GDPR;
- Prevent Duty guidance;
- Teaching online safety in schools (DfE);
- Relationships Education, Relationships and Sex Education and Health Education guidance;
- Searching, screening and confiscation guidance;
- Department for Education Filtering and Monitoring: core standard;
- relevant guidance on cyber-bullying, online abuse, image-sharing and artificial intelligence.

This policy should be read alongside the school's safeguarding and child protection policy and other relevant school policies listed in section 14.

Roles and responsibilities

Governing body

- maintains strategic oversight of online safety;
- ensures appropriate filtering and monitoring arrangements are in place and reviewed;
- ensures staff receive appropriate safeguarding and online safety training;
- receives assurance about significant online safety concerns, trends and actions;
- ensures this policy is reviewed at least annually.

Headteacher / senior leaders

- ensure the policy is implemented and understood;
- ensure online safety is included within safeguarding arrangements and school improvement activity;
- work with the DSL and IT support to review filtering, monitoring and online risks;
- ensure appropriate action is taken when online safety concerns arise;
- ensure staff know how to report technical or safeguarding concerns.

Designated Safeguarding Lead (DSL)

- leads on safeguarding and online safety as part of the school's safeguarding arrangements;
- responds to safeguarding concerns identified through filtering, monitoring or reports from pupils, staff or families;
- maintains appropriate records of significant online safety concerns;
- works with IT support and senior leaders to understand filtering and monitoring reports;
- ensures concerns are referred or escalated in line with safeguarding procedures.

IT support

- maintains the school's filtering, monitoring and security systems;
- provides appropriate reports and support to senior leaders and the DSL;
- investigates and addresses technical concerns and system failures;
- works with the school to check that new devices and services are appropriately configured before use.

All staff

- follow this policy and the relevant Acceptable Use Agreement;
- model safe, respectful and responsible use of technology;
- report online safety and safeguarding concerns promptly;
- do not attempt to bypass filtering or monitoring controls;
- use school systems and devices appropriately and protect passwords and personal information.

Pupils

Pupils are expected to follow the school's Acceptable Use Agreement, use technology respectfully, keep personal information safe and tell a trusted adult if something online makes them worried, uncomfortable or unsafe.

Parents and carers

Parents and carers are encouraged to support the school's approach, talk regularly with children about their online lives and report concerns to the school where appropriate.

Educating pupils about online safety

Online safety education is part of the curriculum and is reinforced through safeguarding, PSHE/RSE, computing and day-to-day teaching. Teaching is age-appropriate and reflects the needs and experiences of our pupils.

- how to recognise unsafe or inappropriate content, contact and behaviour;
- how to protect personal information, accounts and passwords;
- how to communicate respectfully and deal with conflict online;
- how to recognise manipulation, pressure, scams and misleading information;
- how to respond to cyber-bullying and other harmful online behaviour;
- how and when to report concerns and seek help;
- the risks associated with sharing images and personal information;
- appropriate and responsible use of social media, games, apps and online services;
- the benefits and risks of artificial intelligence and how to use AI critically and safely.

Staff will reinforce the message that pupils should not be expected to manage a serious online safety concern alone. They should tell a trusted adult.

Educating parents and carers

The school will provide information and signposting to help parents and carers support children's online safety. This may include information about parental controls, age restrictions, social media, gaming, online communication, image-sharing, scams and emerging technologies.

Parents and carers should contact the school if an online incident is affecting a child's safety, wellbeing, relationships or ability to learn. Where appropriate, concerns will be managed through the school's safeguarding, behaviour or anti-bullying procedures.

Cyber-bullying and online behaviour

Cyber-bullying includes bullying carried out through phones, messaging services, social media, games, websites or other digital platforms. The school will treat online bullying seriously whether it occurs during or outside the school day when it affects pupils or the school community.

- reports will be listened to and recorded appropriately;
- evidence such as messages or screenshots may be retained where safe and appropriate;
- the school will assess safeguarding and welfare risks and take proportionate action;
- support will be provided to pupils affected;

- parents/carers will be involved where appropriate;
- serious safeguarding concerns will be referred through the school's safeguarding procedures.

The school will not encourage pupils or families to retaliate online. Staff will provide advice about blocking, reporting and preserving evidence where appropriate.

Acceptable use of technology

School technology, internet access, accounts and devices are provided to support learning and school business. Users must use them safely, legally and respectfully.

Users must:

- keep passwords and login information secure;
- only access material appropriate to their role and age;
- respect other people's privacy and personal information;
- report inappropriate content, safeguarding concerns, cyber-bullying or technical problems;
- follow copyright and licensing requirements;
- take care of school equipment.

Users must not:

- attempt to bypass filtering, monitoring or other security controls;
- access, create or share illegal, discriminatory, abusive, threatening or otherwise inappropriate material;
- share another person's personal information or images without appropriate permission;
- use school systems to bully, harass or intimidate others;
- install software or applications without authorisation;
- use another person's account or credentials.

The school may restrict or withdraw access to devices or systems where there are concerns about misuse. Disciplinary or safeguarding action may be taken where appropriate.

Mobile phones and personal devices

Pupils should not use mobile phones or other personal smart devices during the school day unless the school has specifically agreed an exception because of an identified need. Where a pupil brings a device to school, it must be switched off/silenced and stored in accordance with the school's arrangements.

The school will make reasonable adjustments where required for pupils with identified needs, including medical or accessibility needs. Any agreed arrangements will be set out clearly for staff and pupils.

Staff should not use personal devices to photograph or record pupils unless this is explicitly permitted by school procedures. School-approved systems should be used for school communication and storage of images or information.

Filtering and monitoring

Barn Croft Primary School has appropriate filtering and monitoring arrangements to help protect pupils and staff from illegal, inappropriate and potentially harmful online content. Filtering is preventative; monitoring is reactive and may generate alerts or reports about activity.

- the governing body has strategic oversight of filtering and monitoring;
- senior leaders, the DSL and IT support work together to manage and review provision;
- staff know how to report concerns about filtering, monitoring or inappropriate content;
- filtering and monitoring provision is reviewed at least annually and following significant changes, new technology, new risks or serious incidents;
- checks and resulting actions are recorded;
- new devices and services are checked before being made available to users;
- the school recognises that no filtering system is 100% effective and maintains supervision, education and reporting arrangements alongside technical controls.

Filtering and monitoring should protect pupils without unreasonably restricting teaching and learning. Different levels of access may be appropriate for pupils, staff and other users.

Where filtering or monitoring identifies a possible safeguarding concern, the DSL will consider and respond to it in line with the school's safeguarding procedures.

Artificial intelligence

The school recognises that artificial intelligence (AI) is increasingly part of the digital environment. AI tools may support teaching, planning and learning where their use has been approved and is appropriate.

- staff must use only school-approved AI tools and follow any school instructions for their use;
- personal, sensitive or confidential information about pupils, families or staff must not be entered into an AI tool unless the school has explicitly approved this and appropriate safeguards are in place;
- AI-generated information must be checked for accuracy, bias and appropriateness before it is relied upon or shared;
- pupils will be taught that AI-generated content can be inaccurate or misleading;
- AI must not be used to create harmful, abusive, discriminatory or inappropriate material;
- the school will consider safeguarding, data protection, copyright and age-appropriateness when introducing AI tools.

Responding to online safety incidents

Any member of the school community can report an online safety concern. Concerns should be reported promptly to the DSL or another member of the safeguarding team where they involve a safeguarding risk.

Concern	Initial action
Inappropriate content or website	Stop using the content; report to a member of staff; IT support/DSL considers whether

	technical or safeguarding action is required.
Cyber-bullying or harmful online behaviour	Report to staff; record relevant information; follow behaviour/anti-bullying and safeguarding procedures as appropriate.
Sexual harassment, sexual images or exploitation	Do not forward or circulate material. Report immediately to the DSL and follow safeguarding procedures.
Threats, abuse or suspected criminal activity	Report immediately to the DSL. The school will consider whether external agencies should be contacted.
Technical or filtering failure	Report to IT support and the relevant senior leader; record significant concerns and actions.
Loss or suspected compromise of an account/device	Report immediately; change credentials or isolate the device where instructed; follow data protection/cyber security procedures.

Staff should not investigate safeguarding concerns independently where doing so could increase risk or interfere with appropriate safeguarding action. The DSL will coordinate the response.

Where an online incident occurs outside school, the school may act where it has a safeguarding, welfare, behaviour or educational impact. Parents/carers may also need to report incidents to the relevant platform or external agency.

Staff training

Online safety is included within safeguarding training and induction. Staff receive information about this policy, Acceptable Use, reporting routes, filtering and monitoring, emerging online risks and relevant safeguarding concerns.

Training is updated when guidance, technology, school systems or identified risks change. Staff are expected to keep their knowledge current and to seek advice where they are unsure.

Monitoring and review

The effectiveness of this policy will be monitored through safeguarding records, incident reporting, filtering and monitoring reviews, staff feedback, pupil voice and other relevant information.

The governing body will receive appropriate assurance about online safety arrangements. The policy will be reviewed at least annually, and sooner if there are significant changes to guidance, technology, school systems or identified risks.

Next scheduled review: September 2027.

Links with other policies

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy

- Data Protection / Privacy arrangements
- Mobile Phone / Personal Device arrangements, where applicable
- Acceptable Use Agreements
- Equality and Inclusion arrangements
- Staff Code of Conduct
- Whistleblowing and Complaints procedures, where relevant

EYFS/KS1 Acceptable Use Agreement

We use computers, tablets and the internet to help us learn. We can have fun and stay safe by:

- telling an adult if something online worries us;
- asking an adult before using a new website, app or online service;
- being kind and respectful when using technology;
- keeping our passwords private;
- not sharing photos or personal information without permission;
- using school devices carefully;
- following instructions from adults.

I understand that school staff may check how school technology is being used to help keep everyone safe.

Child name: _____ Class: _____

Child signature: _____ Date: _____

Parent/carer signature: _____ Date: _____

Appendix 2: KS2 Acceptable Use Agreement

When using school technology, I agree that I will:

- use technology for the purpose my teacher has given me;
- keep passwords and login details private;
- tell an adult if I see something upsetting, unsafe or inappropriate;
- communicate respectfully and not bully, threaten or harass others;
- not share personal information, images or other people's work without permission;
- not attempt to bypass filtering or security controls;
- not download or install software without permission;
- respect copyright and acknowledge sources where required;
- use AI tools only when my teacher/school has said they may be used and check AI-generated information carefully;
- remember that school systems may be monitored to help keep users safe.

Pupil name: _____ Class: _____

Pupil signature: _____ Date: _____

Parent/carer signature: _____ Date: _____

Appendix 3: Staff, governors, volunteers and visitors Acceptable Use Agreement

I agree to use school technology, systems and information responsibly and in accordance with school policies.

- I will protect passwords, accounts, devices and confidential information.

- I will use school-approved systems for school communication and storage of pupil information.
- I will not access, create, store or share inappropriate or illegal material using school systems.
- I will not attempt to bypass filtering, monitoring or security controls.
- I will report safeguarding concerns, inappropriate content, cyber incidents and technical failures promptly.
- I will not use personal devices to photograph or record pupils unless permitted by school procedures.
- I will not enter confidential or personal information into AI tools unless explicitly authorised and appropriate safeguards are in place.
- I understand that school systems may be monitored and that misuse may result in action under relevant school procedures.

Name: _____ Role: _____

Signature: _____ Date: _____

Appendix 4: Online Safety Incident Log

Date/time	Person reporting	Pupil/user(s)	Nature of concern	Immediate action	DSL/IT action	Outcome/follow-up

For safeguarding concerns, the school's safeguarding recording system should be used as the main record where appropriate. This log is intended to support recording of online safety/technical incidents and actions.