Bushfield Road Infant School

Online Safety Policy

Approval date: November 2026
Review date: November 2027

1. Purpose and principles

At Bushfield Road Infant School, online safety is part of safeguarding. We want pupils to benefit from technology for learning while being protected from harm and taught how to use it safely in ways appropriate to their age.

Our approach reflects our values:

- **Kindness:** pupils and adults communicate respectfully and do not use technology to hurt, frighten or exclude others.
- **Teamwork:** staff, governors, families and our IT support work together to keep pupils safe.
- **Curiosity:** pupils learn to explore digital resources safely, think carefully about what they see and hear, and ask for help.

This policy applies to pupils, staff, governors, volunteers, visitors and contractors using school devices, networks, accounts or online services. It also applies to staff conduct online where this could affect pupils' safety or the school's professional responsibilities.

Online safety risks include the four areas set out in *Keeping Children Safe in Education*:

- **Content:** seeing illegal, inappropriate or harmful material.
- **Contact:** harmful interactions with other people or generative AI tools, including grooming, pressure or exploitation.

- **Conduct:** online behaviour that causes or increases harm, such as bullying, sharing images or personal information, or unsafe use of technology.
- **Commerce:** scams, phishing, inappropriate advertising, online gambling or other financial risks.

Online risks can arise on school or personal devices, and on or off school premises. Relevant concerns will be handled through the school's safeguarding procedures.

2. Roles and responsibilities

Governing body

The governing body will:

- ensure online safety is included in the school's safeguarding arrangements;
- ensure appropriate filtering and monitoring systems are in place;
- receive assurance that those systems are reviewed and concerns acted upon;
- identify a governor to have oversight of filtering and monitoring arrangements.

Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team (SLT) will:

- implement this policy and ensure staff know how to report concerns;
- oversee the school's filtering and monitoring arrangements;
- ensure responsibilities are assigned and staff receive suitable training;
- ensure that online safety incidents and decisions are followed up and recorded.

The SLT member responsible for filtering and monitoring will lead the annual effectiveness review, supported by the DSL and IT support, and ensure that checks and actions are recorded.

Designated Safeguarding Lead

The DSL will:

- lead on online safety as part of the school's safeguarding work;
- consider online concerns, decide on safeguarding actions and make referrals where needed;
- support the annual filtering and monitoring review;
- ensure relevant concerns, decisions and outcomes are recorded in the school's safeguarding system.

Staff, volunteers, visitors and contractors

All adults must:

- follow this policy and the relevant acceptable use agreement;
- supervise pupils appropriately when they use technology;
- report concerns promptly to the DSL or a deputy DSL;
- use school-approved accounts, devices and services for school purposes;
- keep passwords and personal data secure.

IT support and service providers

The school's IT support and service providers will support the school in maintaining and reviewing systems in line with agreed arrangements. Technical support does not replace the school's safeguarding responsibilities.

Pupils and parents or carers

Pupils will be taught age-appropriate ways to use technology safely, treat others kindly, protect personal information and tell a trusted adult if something online worries them.

Parents and carers are encouraged to talk with their child about safe technology use at home and to contact the school if an online concern affects their child's welfare or school life.

3. Filtering and monitoring

The school uses **NetSweeper for internet filtering**. **SLT oversees the school's filtering and monitoring arrangements**, working with the DSL and IT support.

The school will ensure that these arrangements are appropriate for the age and needs of its pupils and for how technology is used at Bushfield Road Infant School. Staff must know how to report concerns about content accessed online, or about filtering or monitoring not working as intended.

At least once every academic year, the SLT member responsible for filtering and monitoring will lead a review, supported by the DSL and IT support. The review will include checks that filtering works appropriately on internet-connected devices in all relevant locations. The school will keep a record of the checks, the review's findings and any actions taken.

The review will consider:

- what the school's systems block, allow and monitor;
- whether filtering works on school-managed devices and networks, including after relevant changes to devices, systems or network arrangements;
- how pupils and staff use technology, including any approved AI tools;
- any safeguarding concerns, incidents, gaps or technical limitations;

- how concerns, alerts and incidents are reported, escalated and followed up;
- whether the arrangements continue to be suitable for pupils' age and needs.

The review will also consider any necessary changes to policies, staff training, curriculum, monitoring or technical arrangements. A review will take place sooner if a safeguarding risk is identified, there is a significant incident or new technology is introduced.

The SLT will agree with NetSweeper and IT support how checks, technical concerns and relevant alerts are reported to the school, and how urgent issues are escalated. Any temporary exception to filtering must be authorised by the Headteacher or delegated senior leader, recorded, time-limited and risk-assessed.

Technical support

The school's 2025 policy names **Wavenet** as its IT service provider. The school should confirm this is still current before approving this policy. The name of the IT provider does not change the SLT's oversight responsibilities or the DSL's role in safeguarding decisions.

4. Teaching pupils to stay safe online

Online safety will be taught in ways suitable for infant-aged pupils and reinforced through everyday classroom practice. Staff will teach pupils to:

- stop and tell a trusted adult if they see, hear or receive something that worries them;
- keep personal information, such as their address and passwords, private;
- understand that people and messages online may not be what they seem;
- use technology kindly and respectfully;
- ask an adult before opening links, using websites or trying a new digital tool;
- understand that pictures, videos and information online may be misleading or upsetting.

In the early years, internet use will be adult-led and closely supervised. Pupils will use teacher-selected resources rather than unrestricted internet access. In Key Stage 1, pupils may use selected online resources for learning with adult supervision and age-appropriate teaching.

Staff will select resources that are suitable for pupils and supervise their use in line with pupils' age, needs and the activity. Online safety teaching should be revisited when relevant concerns arise, and not confined to a single annual lesson.

5. Generative AI and new technology

Staff must not introduce pupil-facing generative AI tools or other new online services without the Headteacher's approval and consideration of safeguarding, privacy, age suitability, filtering and monitoring.

Pupils must not use open-access AI tools independently in school. Any approved use must be adult-led, age-appropriate and closely supervised. Staff must follow school guidance on AI and must not enter identifiable pupil information, confidential information or safeguarding information into public AI services.

6. Staff and adult use of technology

Adults must maintain professional boundaries online. Staff and volunteers must not:

- contact pupils or their families through personal social media or personal messaging accounts in a professional capacity;
- invite pupils to personal social media accounts or share personal contact details with them;
- use personal devices to photograph or record pupils;
- post identifiable information or images of pupils online;
- use school systems to access, store or share illegal, offensive, discriminatory or unrelated material.

Staff must use school-approved methods to communicate with families. If a member of staff needs to use a personal phone for an approved work purpose, they must follow the school's agreed procedure to protect their number and the privacy of pupils and families.

Any concern about an adult's online conduct must be reported through the school's safeguarding or allegations procedures. A concern about the Headteacher must be reported to the appropriate alternative contact under those procedures.

7. Devices, photographs and personal information

Only school-approved devices and accounts may be used for school activity, unless the Headteacher has authorised an exception. Staff must not use personal phones or cameras to take images or recordings of pupils.

Images or videos of pupils may be taken or shared only for an authorised school purpose and in line with the school's consent arrangements. Staff must use approved storage and sharing systems, avoid including pupils' full names with published images and follow the school's data protection requirements.

Staff must protect passwords and log out of systems when they are no longer in use. Any suspected loss of a device, account compromise, accidental disclosure or other data breach must be reported promptly to the Headteacher and the relevant school lead.

8. Mobile phones and personal devices

Pupils must not use personal mobile phones, smart watches or other internet-enabled personal devices in school unless the Headteacher has agreed an exception for a specific need.

Staff personal phones and devices must not be used in lessons or while supervising pupils. Personal devices should be kept in the designated staff area or stored securely in line with school arrangements. Staff must not use personal devices to photograph, record or communicate with pupils.

9. Responding to online safety concerns

Any pupil who is worried by something online should be listened to calmly and reassured that they did the right thing by telling an adult. Staff must not promise secrecy.

Staff must:

1. Make sure the pupil is safe and tell the DSL or deputy DSL promptly.
2. Record the concern factually in the school's safeguarding system, including what was reported, actions taken, decisions and outcomes.
3. Preserve relevant information where safe and appropriate, without forwarding, copying or unnecessarily viewing harmful material.
4. Follow the DSL's direction on parent or carer communication, referrals and further action.

The DSL will decide whether the concern needs a safeguarding response, contact with parents or carers, referral to children's social care or the police, or support from the school's IT provider. Staff must not investigate a safeguarding concern themselves or delay passing it to the DSL.

Concerns about online bullying, harmful messages or inappropriate contact must also be addressed under the school's safeguarding and behaviour procedures. Concerns about an adult must be handled through the school's allegations procedures.

10. Staff training and communication

All staff will be made aware of this policy and how to report an online safety concern. Online safety will be included in safeguarding training and induction for new staff, volunteers and relevant contractors.

Pupils will receive age-appropriate teaching and reminders. The school will share clear information with parents and carers about pupils' use of technology, the school's expectations and how to raise concerns.

11. Review

The Headteacher and DSL will review this policy at least annually and sooner following a significant incident, a change in technology or relevant guidance, or a review of filtering and monitoring arrangements. The annual online safety review will be supported by a risk assessment that considers the risks pupils may face.