BREWSTER AVENUE INFANT AND NURSERY SCHOOL

ONLINE SAFETY POLICY

This policy is adapted from the SWGfL Model Policy

This policy applies to all members of the school community (including staff, children, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

This policy was ratified by the Full Governing Body on 9th July 2026

Date for review (this policy will be reviewed every two years): Summer 2028

Contents

Responsibilities 2
Acceptable use 4
Reporting concerns 4
Use of Artificial Intelligence (AI) 5
Teaching and Learning 5
Staff training 6
Filtering and Monitoring 6
Technical Security 6
Cyber Security 7
Data Protection 7
Public Online Communications 7

This Online Safety Policy sets out how Brewster Avenue Infant School will safeguard members of our community online, in line with statutory guidance and best practice**.** It should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection policies.

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Ensure that all staff access relevant training and are able to fulfil their roles.
- Work with governors and IT provider on filtering and monitoring.
- Work with curriculum leaders to map, embed and evaluate online safety education.

Governors

Governors approve the Online Safety Policy and challenge its effectiveness, in line with KCSIE expectations, including

- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, in line with DfE standards.
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Support parent/carer and community engagement in online safety.

Curriculum Leaders

Curriculum leads will work with the DSL to deliver a planned online safety programme through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy and Safeguarding/Child Protection Policy and sign/comply with the Staff Acceptable Use Agreement.

- Maintain professional boundaries (including online/remote learning).
- Supervise children's use of technology and follow procedures for reporting online safety issues.
- Embed online safety in the classroom.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards, although the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with DSL.
- Monitor systems for misuse and report concerns promptly to the Headteacher.
- Follow the school's Online Safety policy and keep technical knowledge current.

Pupils

Pupils will:

- Follow the school rules for using technology and the internet.
- Tell an adult of they have any problems or worries when using IT.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour and will be encouraged to reinforce safe online behaviour at home. The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home, including by:

- Publishing the Online Safety Policy on the school website
- Providing guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Sharing updates through meetings (e.g. Year 2 Café), newsletters and campaigns.

Community users

Community users accessing school systems or platforms will sign a Community User Acceptable Use Agreement before access is provided. The school welcomes partnership working and shares good practice where appropriate.

Acceptable use

An Acceptable Use Agreement is a set of rules that defines what users are permitted to do when accessing the schools IT systems, networks, or digital resources, with the aim of safeguarding pupils, maintaining cyber security and protecting data. All users of school based hardware or digital technology are required to sign the relevant AUA prior to being granted access.

Reporting concerns

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns.

Concerns can be raised by any member of the school community including pupils, staff, governors, parents/carers, and volunteers. Reporting processes are aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.

Concerns can be shared by speaking to a member of staff or sending an email to the school office. All online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.
- A secure and confidential record of all incidents is kept, including actions, decisions, and follow-up.

Where online safety concerns or incidents occur outside school and are known to the school, we will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Provide training and guidance for staff on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping children understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools (Microsoft Co-Pilot, Arbor AI) may be used for schoolwork, and staff should use log into school-provided accounts to support oversight and reduce risk.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

Teaching and Learning

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all children. Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including PSHE and Computing).

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;

- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools.

Where internet use is planned, children are guided to appropriate resources and supported if unsuitable content is encountered.

Staff training

In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., DfE Technical Standards, KCSIE) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring)

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering, including when used off-site
- staff and children understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering)
- no system is relied upon in isolation; reporting routes and professional judgement remain central.

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack

- incidents and weaknesses are reported, recorded and used to inform improvement

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents.

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. See Data Protection Policy and Privacy Statements for more information.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks e.g. via the school website. The school ensures that public online communications are appropriate, accurate and well-managed. To reduce the risk of illegal manipulation, images of staff and children's faces are not routinely used. If there was a specific requirement e.g. for a newspaper report, specific consent would be sought.