



ONLINE SAFETY POLICY

DECEMBER 2025

Details

Title: Online Safety Policy

Approved: December 2025

Next Review: December 2026

Approved by: Proprietor Body

Date	Section Amended	Signature

1. Policy Aims

This policy aims to:

- Safeguard and protect students, particularly those with autism, from the multifaceted risks associated with online activity, including exposure to harmful content, inappropriate contact, and engaging in risky conduct.
- Ensure the school meets its statutory duties under the Independent School Standards (ISS), specifically Part 3: Welfare, health and safety of pupils, and Part 2: Spiritual, moral, social and cultural development of pupils.
- Promote responsible digital citizenship among students and staff, fostering a culture of safe, respectful, and positive online engagement.
- Provide clear, accessible, and comprehensive guidance for staff, pupils, parents, and carers on the safe, responsible, and lawful use of digital technology, both within and outside school.
- Ensure that online safety is an integral part of the school's overall safeguarding arrangements.

2. Legal Framework

This policy is guided by and complies with all relevant legislation and statutory guidance, including, but not limited to:

- The Health and Safety at Work etc. Act 1974
- The Education (Independent School Standards) Regulations 2014
- The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- The Voyeurism (Offences) Act 2019
- The Malicious Communications Act 1988
- The Communications Act 2003
- The Children Act 1989 and 2004
- DfE 'Keeping children safe in education' (KCSIE)
- DfE 'Teaching online safety in school'
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education' (where applicable)
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World - 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

3. Scope

This policy applies to:

- All staff (including teaching, support, administrative, and peripatetic staff), pupils, volunteers, contractors, and visitors.
- All devices connected to the school's network and all school-managed systems (e.g., email, learning platforms, cloud services).
- All online activities that take place on school premises, using school equipment, or during school-organised off-site activities.
- Off-site activities where pupils are using technology provided by or connected to the school.
- Behaviour outside of school that impacts the safety or wellbeing of pupils or staff, or brings the school into disrepute.

4. Context - Autism-Specific Considerations

Given the unique vulnerabilities associated with autism, such as challenges in interpreting social cues, understanding abstract concepts, literal interpretation of language, potential for heightened anxiety, and increased risk of online exploitation or bullying, this policy prioritises:

- Structured, explicit teaching of online safety concepts, using concrete examples and clear rules.
- Use of visuals, social stories, and simplified language to reinforce safe behaviours and understanding of online risks.
- Proactive, age and need-appropriate filtering and monitoring tailored to cognitive and developmental needs.
- Emphasis on direct communication and clear reporting pathways for pupils who may struggle to express concerns verbally.

5. Roles and Responsibilities

5.1. The Proprietor/Governing Body

The Proprietor/Governing Body is responsible for:

- Holds ultimate legal accountability for the school's compliance with Independent School Standards (ISS) and safeguarding legislation
- Ensures the school is sufficiently resourced to maintain filtering and monitoring standards

5.2. The Local Governing Committee (LGC)

- Formally approves and reviews the school-specific Online Safety Policy

- Monitors implementation by undertaking regular visits and reviewing the Principal's termly reports on safeguarding / online monitoring
- Provides robust support and challenge to leaders regarding the impact of the online safety curriculum
- Ensuring effective filtering and monitoring systems are in place and reviewed annually.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and regularly thereafter.

5.3. The Principal

The Principal is responsible for:

- The overall implementation and day-to-day management of this policy.
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including curriculum and safeguarding.
- Supporting the DSL by ensuring they have sufficient time and resources to carry out their online safety responsibilities.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training.
- Ensuring online safety practices are audited and evaluated regularly.
- Organising engagement with parents to keep them up-to-date with current online safety issues.
- Working with the DSL and ICT support to conduct light-touch reviews of this policy
- Reports directly to the LGC on the effectiveness of online safety practices
- Shares data and incident logs with the LGC to enable them to monitor and scrutinise how policies work in practice

5.4. The Designated Safeguarding Lead (DSL) and Deputy DSLs

The DSL has lead responsibility for online safety in the school and is responsible for:

- Undertaking training to understand the risks associated with online safety, including additional risks faced by pupils with SEND.
- Liaising with relevant staff (e.g., SLT, ICT support) on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies (e.g., police, children's social care, CEOP) as required.
- Working closely with the police during investigations.
- Keeping up-to-date with current research, legislation, and online trends.
- Coordinating the school's participation in online safety events (e.g., Safer Internet Day).

- Establishing and communicating clear procedures for reporting online safety incidents and inappropriate internet use by both pupils and staff.
- Maintaining records of reported online safety concerns and actions taken.
- Monitoring online safety incidents to identify trends and gaps in provision.
- Understanding the filtering and monitoring processes in place and ensuring staff are trained on them.

5.5. ICT Support (Internal or External)

The ICT Support is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures.
- Ensuring that the school's filtering and monitoring systems are updated and effective.
- Regularly checking firewalls and network security.
- Managing user privileges and password security.

5.6. All Staff Members

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours and maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues and understanding indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Adhering to the Staff Acceptable Use Agreement.

5.7. Pupils

Pupils are responsible for:

- Learning and following the school's online safety rules, with support as required.
- Reporting any online content or contact that makes them feel uncomfortable, worried, or unsafe to a trusted adult (parent/carers or school staff).
- Adhering to the Acceptable Use Agreement.

5.8. Parents/Carers

Parents/Carers are responsible for:

- Engaging with school guidance and supporting their child's safe use of technology at home.

- Monitoring their child's online activity at home and implementing appropriate parental controls.
- Reporting any online safety concerns involving their child or other pupils to the school.

6. Managing Online Safety Risks (The 4 Cs)

The school's approach to online safety is structured around the four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material (e.g., pornography, fake news, self-harm and suicide, discriminatory or extremist views).
- **Contact:** Being subjected to harmful online interaction with other users (e.g., peer pressure, commercial advertising, adults posing as children or young adults with the intention to groom or exploit children).
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm (e.g., sending and receiving explicit messages, cyberbullying, sharing of nudes/semi-nudes).
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing, and/or financial scams.

Measures are implemented across all areas to protect pupils and staff.

7. Education and Training

7.1. Staff Training

Annual online safety training is integrated with safeguarding CPD for all staff, covering:

- Recognising online risks, including grooming, exploitation, radicalisation, and harmful online challenges.
- Understanding the specific vulnerabilities of pupils with autism and how to support them.
- Responsibilities related to filtering and monitoring systems.
- Reporting procedures for online safety incidents.
- Professional conduct and social media use.
- Regular updates are provided on new online safety information, guidance, and legislation.

7.2. Pupil Education

- Online safety is embedded throughout the curriculum, particularly in PSHE, and Computing
- Teaching is tailored to pupils' ages, developmental stages, and specific needs (e.g., through bespoke autism-focused sessions, visual aids, social stories).

Pupils are taught:

- How to evaluate online content and recognise persuasion techniques.
- What healthy and respectful online relationships look like.
- Body confidence, self-esteem, and consent regarding image sharing.

- Acceptable and unacceptable online behaviour.
- How to identify online risks and when something is deceitful or harmful.
- How and when to seek support from a trusted adult.

7.3 Parent/Carer Engagement

- The school works in partnership with parents/carers to ensure pupils stay safe online at school and at home.

Parents/carers are provided with information about:

- The school's approach to online safety.
- Various online risks (e.g., grooming, cyberbullying, inappropriate content).
- Ways to prevent access to harmful content at home (e.g., parental controls).
- This information is disseminated through workshops, newsletters, the school website, and signposting to reputable online safety resources (e.g., NSPCC, UK Safer Internet Centre, CEOP).

8. Acceptable Use Agreements (AUAs)

The school provides a clear, accessible Acceptable Use Agreement

9. Filtering and Monitoring

- The school's ICT network has age- and need-appropriate filtering and monitoring systems in place, meeting the DfE's 'Filtering and monitoring standards for schools and colleges'.
- The DSL and ICT Support ensure that 'over-blocking' does not unreasonably restrict educational content.
- Active supervision and monitoring of device usage and online activity are conducted, with device logs and safeguarding alerts flagged to the DSL.
- All users of the network and school-owned devices are informed about how and why their online activity is monitored.
- Concerns identified through monitoring are reported to the DSL and managed in line with the Child Protection and Safeguarding Policy.
- Deliberate breaches of the filtering system by pupils will result in disciplinary action in line with the Behaviour Policy. For staff, such breaches will be managed under the Disciplinary Procedure
- Any material believed to be illegal, accessed inadvertently or deliberately, will be reported immediately to the appropriate agency (e.g., Internet Watch Foundation (IWF), CEOP, police).

10. Responding to Online Incidents

10.1. Reporting Concerns

- All online safety concerns, however minor, must be reported immediately to the DSL or a Deputy DSL.
- Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing and will be vigilant for indicators of online harm.
- Confidentiality cannot be promised where there is a safeguarding concern, and information may be shared lawfully if necessary to protect the child.

10.2. Incident Management

- All concerns are logged and escalated via the school's safeguarding procedures.
- Support is personalised, involving SEN staff and the DSL, to reflect the needs of autistic pupils, ensuring a sensitive and appropriate response.
- External agencies (e.g., police, social care, CEOP) are involved as necessary.
- The school avoids unnecessarily criminalising pupils where criminal behaviour is thought to be inadvertent and a result of ignorance or normal developmental curiosity.
- Concerns regarding a staff member's online behaviour are reported to the Principal (or Chair of Governors if concerning the Principal) and managed in line with the Staff Code of Conduct and Disciplinary Policy.
- Concerns regarding a pupil's online behaviour are reported to the DSL and managed in accordance with relevant policies (e.g., Behaviour Policy, Child Protection and Safeguarding Policy).

10.3. Specific Online Harms

The school has clear procedures for addressing specific online harms:

- Cyberbullying: Not tolerated under any circumstances. Incidents are dealt with quickly and effectively in line with the Anti-bullying Policy / Child on Child Abuse Policy.
- Child-on-Child Sexual Abuse and Harassment: All staff are aware of examples (e.g., upskirting, sexualised bullying, sharing indecent images) and promote a zero-tolerance approach. Concerns are reported to the DSL and managed in line with the Child-on-Child Abuse Policy and Child Protection and Safeguarding Policy.
- Grooming and Exploitation (CSE/CCE): Staff are trained to recognise indicators of grooming and exploitation. Concerns are reported to the DSL and managed in line with the Child Protection and Safeguarding Policy.
- Radicalisation: Staff are aware of factors that increase vulnerability to radicalisation online. Concerns are reported to the DSL and handled in line with the Prevent Duty Policy.
- Mental Health: Staff understand the impact of online activity on mental health. Training is provided on recognising indicators of mental health challenges related to online use.
- Online Hoaxes and Harmful Online Challenges: Where suspected, these are reported immediately to the DSL, who assesses the risk and determines a proportionate, supportive, and age-appropriate response, in line with DfE guidance.
- Cyber-crime: The school educates pupils on lawful technology use and considers referrals to programmes like Cyber Choices for pupils at risk of involvement in cyber-crime.

11. Use of Devices

11.1. School-Owned Devices

- School-owned devices (laptops, tablets, etc.) are issued to staff and pupils to support teaching and learning.
- These devices are used in accordance with the Acceptable Use Agreement.
- All school-owned devices are password protected, fitted with remote access software for data protection, and regularly reviewed for software updates and inappropriate material.
- No unauthorised software or apps can be downloaded onto school-owned devices.
- Misuse of school-owned devices by staff or pupils will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

11.2. Personal Devices (BYOD)

- Personal devices (e.g., mobile phones, smartwatches) are generally **not permitted for pupil use on the school site** during school hours.
- Staff use of personal devices is governed by the Bring Your Own Device Policy and Staff Code of Conduct. Staff are not permitted to use personal devices in classrooms during teaching time or to take photos/videos of pupils.
- Personal devices connecting to the school network must be checked by ICT Support for security.
- Concerns about staff or visitors' use of personal devices on school premises are reported to the Principal or DSL. Illegal content found on personal devices will result in police involvement and disciplinary action.

12. Remote Learning

- All remote learning is delivered in line with the Acceptable Use Policy
- The school risk assesses technology used for remote learning to ensure privacy and prevent inappropriate use.
- School-owned equipment used for remote learning has suitable anti-virus software and secure connections.
- The school maintains regular contact with parents during remote learning to reinforce online safety, inform them of online activities, and encourage parental controls.

13. Network Security

- Technical security features, such as anti-virus software and firewalls, are kept up-to-date and managed by ICT Support.
- Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments and must report all malware/virus attacks.

- User privileges are differentiated based on role, and all user accounts are password protected with regular password changes.
- The school's network is monitored for inappropriate and malicious content.

14. Emails

- Access to and use of school email accounts are managed in line with the Data Protection Policy, Acceptable Use Policy, and Staff Code of Conduct.
- Staff and pupils are given approved school email accounts for school-related work only. Personal email accounts are not permitted on the school site.
- Sensitive or personal information is only sent via secure and encrypted email.
- Users are required to block spam and report suspicious emails to ICT Support.
- The school monitoring system detects inappropriate links, malware, and profanity in emails.

15. Social Networking

- **Personal Use:** Access to social networking sites is filtered. Staff and pupils are not permitted personal social media use during lesson time. Staff are advised that their conduct on social media can impact their professional role and reputation. Staff will not engage in inappropriate contact with pupils or their families on social media.
- **School Use:** Official school social media channels are used only for educational or engagement purposes, managed by authorised staff

16. The School Website

- The Principal is responsible for the overall content of the school website, ensuring it is appropriate, accurate, up-to-date, and meets DfE and KCSIE requirements.
- The website complies with guidelines for publications, including accessibility, data protection, intellectual property rights, privacy policies, and copyright law.

17. Monitoring and Review

This policy will be reviewed and approved every year by the Local Governing Committee



Bart's Training & Support Alliance

St. Bart's Multi-Academy Trust

c/o Belgrave St Bartholomew's Academy,
Sussex Place, Longton, Stoke-On-Trent, Staffordshire, ST3 4TP
www.sbmat.org T: 01782 486350
