



BRADFORD ACADEMY
TRUST



Our Vision
RESPONSIBILITY
RESPECT
RESILIENCE

**A shining light in our
community**

You are the light of the world. A city
on a hill cannot be hidden. - Matthew
5:14b

Online - Safety Policy

Approved by:	Board	Date: December 2024
Last reviewed on:	November 2024	
Next review due by:	November 2025	
Related Documents	• POLES • Social Media Policy (POLPB) • Equal Opportunities Policy (POLEO) • Online Bullying Policy	
Guidance	Protocol for responding to Online safety incidents, Protocol for Data Security & Search and Confiscation guidance from DfE	
Author	Jen Jakes (Primary Principal)/Mark Berry (Information Systems Director)	

Contents

1. Introduction and Overview	3
2. Education and Curriculum	8
3. Expected Conduct and Incident Management	10
4. Managing the IT and Computing Infrastructure	12
5. Data Security: Management Information System Access and Data Transfer	16
6. Equipment and Digital Content	18

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents)
4. Protocol for responding to Online safety incidents
<https://www.lgfl.net/online-safety/resource-centre?a=3> - handling infringements
5. Search and Confiscation guidance from DfE
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out key principles for the use of IT-based technologies by all members of the Bradford Academy community.
- Safeguard and protect children and staff.
- Assist staff in working safely and responsibly with the Internet and other communication technologies.
- Set clear expectations for responsible Internet use for educational, personal, or recreational purposes.
- Establish structures to address online abuse, such as online bullying, in alignment with other Academy policies.
- Ensure all community members understand that unlawful or unsafe behaviour is unacceptable and may result in disciplinary or legal action.
- Minimize the risk of misplaced or malicious allegations against adults working with students.

Main Areas of Risk

Content:

- Exposure to inappropriate content (e.g., online pornography, violent games, substance abuse)
- Lifestyle websites promoting harmful behaviours (e.g., pro-anorexia, self-harm, suicide)
- Hate sites
- Content validation (checking authenticity and accuracy)

Contact:

- Grooming
- Online bullying
- Identity theft and password sharing

Conduct:

- Privacy issues (disclosure of personal information)
- Digital footprint and online reputation
- Health and well-being (time spent online)
- Sexting (sending/receiving intimate images)
- Extremism
- Copyright infringement (music, film)

Scope

This policy applies to all members of the Bradford Academy community (staff, students, governors, volunteers, parents, visitors, community users) who access and use Academy IT systems, both on and off-site.

The Education and Inspections Act 2006 empowers Headteachers/Principals to regulate student behaviour off-site and impose disciplinary penalties for inappropriate behaviour. This includes online bullying and other online safety incidents linked to Academy membership. The 2011 Education Act extends these powers to search electronic devices and delete data. Actions can only be taken for issues covered by the published Behaviour Policy.

Bradford Academy will handle such incidents according to this policy and related behaviour and anti-bullying policies, informing parents/carers of known incidents of inappropriate online behaviour occurring outside the Academy.

Role	Key Responsibilities
Principal	• Overall responsibility for Online Safety provision and data security (SIRO) • Ensure use of an approved, filtered Internet Service • Ensure staff receive suitable training for Online Safety roles • Be aware of procedures for serious online safety incidents • Receive regular monitoring reports from the Online Safety Coordinator/Officer • Monitor and support staff handling internal Online Safety procedures
Online Safety Co-ordinator / Designated Child Protection Lead	• Manage day-to-day Online Safety issues • Lead in establishing and reviewing Online Safety policies • Promote Online safeguarding awareness • Embed Online Safety education across the curriculum • Liaise with IT Support staff • Communicate with SLT and Online Safety Governor • Ensure staff follow procedures for Online Safety incidents • Maintain an Online Safety incident log • Facilitate training and advice for staff • Liaise with Local Authority and relevant agencies • Stay updated on Online Safety issues and legislation
Governors / Online safety governor	• Ensure adherence to Online Safety advice • Approve and review the Online Safety Policy • Encourage parent and community engagement in Online Safety activities • Regularly review Online Safety logs with the Coordinator/Officer

Role	Key Responsibilities
Computing Curriculum Leader	• Oversee delivery of Online Safety in the computing curriculum • Liaise regularly with the Online Safety Coordinator
Information Systems Director/Manager	• Report Online Safety issues to the Coordinator • Enforce password protection policies • Ensure misuse detection and virus protection • Secure the IT system • Implement access controls and encryption • Apply and update web filtering policies • Inform BLN of filtering issues • Monitor network and system use • Ensure backup procedures • Maintain documentation of security procedures
Data Protection Officer	• Ensure compliance with Data Protection laws • Assess data transfers • Approve new software using staff/student/parent data • Handle Subject Access and FOI requests
Data Manager	• Ensure appropriate access controls for pupil data
Teachers	• Embed Online Safety in the curriculum • Supervise pupils in online activities • Teach research skills and copyright laws
All staff	• Promote and adhere to Online Safety policies • Be aware of issues related to mobile phones, cameras, and handheld devices • Report suspected misuse • Model safe and professional behaviour • Use digital communications professionally
Pupils	• Adhere to the Acceptable Use Policy • Understand research skills and copyright regulations • Report abuse or misuse • Follow policies on mobile phones, cameras, and online bullying • Practice good Online Safety outside the Academy • Learn about Internet benefits and risks • Help create/review Online Safety policies
Parents/Carers	• Support Online Safety and endorse the Acceptable Use Agreement • Promote the Pupil Acceptable Use Agreement • Access Academy systems according to policies • Consult the Academy with concerns about technology use

Role	Key Responsibilities
External groups	Access the network through a segregated, filtered connection for necessary resources

Communication

The policy will be communicated to staff, pupils, and the community in the following ways:

- Posted on the Bradford Academy website and Learning Platform.
- Included in the Bradford Academy staff handbook for new staff.
- Discussed with pupils at the start of each year through Acceptable Use Agreements.
- Issued to the entire Bradford Academy community, typically upon entry.
- Held in pupil and personnel files.

Handling Complaints

- Bradford Academy will take all reasonable precautions to ensure online safety. However, due to the international scale and dynamic nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on Academy devices. Neither Bradford Academy nor the Bradford Learning Network can accept liability for accessed material or any consequences of Internet access.
- Staff and pupils are informed about infringements and possible sanctions, which may include:
 - Interview/intervention by school staff
 - Informing parents or carers
 - Removal of Internet, email, or computer access (potentially affecting access to files, including exam coursework)
 - Referral to the Police (including anti-terrorism)
 - Referral to Children Social Care
- Complaints about staff misuse should follow procedures in the Staff Handbook.
- Complaints of online bullying are handled according to the Anti-Bullying Policy. Child protection-related complaints are handled according to Bradford Academy child protection procedures.

Review and Monitoring

- The Online Safety policy is referenced in other Bradford Academy policies: Computing AUP, Child Protection, Anti-Bullying, Development Plan, Behaviour, PSHE, and Citizenship.
- An Online Safety Coordinator is responsible for document ownership, review, and updates.
- The policy will be reviewed annually or when significant technological changes occur.

- The policy has been approved by the Online Safety Committee and governors, ensuring it is current and appropriate.
- There is widespread ownership of the policy, agreed upon by SLT, governors, and other stakeholders. Amendments will be discussed in detail with all teaching staff.

Version Control

To maintain the Online Safety policy, revisions will be documented. The document owner must ensure the policy includes the following information and that all revisions are stored centrally for audit purposes.

2. Education and Curriculum

Pupil Online Safety Curriculum

Bradford Academy has a structured Online Safety education program within the ICT curriculum, covering skills and behaviours suitable for different ages and experiences, including:

- **STOP and THINK before CLICKING**
- **Evaluate and verify information** before accepting its accuracy
- **Recognize bias or purpose** in web content
- **Refine search techniques**
- **Understand search engines** and their impact on results
- **Practice acceptable online behaviour** (politeness, no abusive language, keeping personal information private)
- **Recognize manipulated photographs** and web content
- **Be cautious with online 'friends'**
- **Avoid sharing personal details** and ensure privacy settings are on
- **Do not post others' pictures/videos** without permission
- **Avoid downloading files** without permission
- **Handle inappropriate materials** appropriately
- **Understand online grooming** risks
- **Recognize and seek help for online bullying, sexting, extremism, and trolling**
- **Report abuse** and seek help from trusted sources (parents, teachers, ChildLine, CEOP button)

Internet Use Planning

- Ensure age-appropriate and curriculum-supportive Internet use
- Remind students of responsibilities via an Acceptable Use Policy displayed throughout the Academy and upon login
- Model safe and responsible technology use by staff
- Educate on plagiarism, copyright, and intellectual property rights
- Address commercial Internet use risks (pop-ups, online buying, gaming, gambling)

Staff and Governor Training

Bradford Academy ensures staff:

- Know how to handle sensitive data securely, including encryption
- Receive regular online safety training as part of safeguarding
- Get e-safeguarding policy and Acceptable Use Policy guidance during induction

Parent Awareness and Training

Bradford Academy provides ongoing advice, guidance, and training for parents through:

- Introduction of Acceptable Use Agreements
- Information via leaflets, newsletters, and the Academy website
- Demonstrations and practical sessions at the Academy
- Safe Internet use suggestions for home
- Information on national support sites for parents

3. Expected Conduct and Incident Management

Expected Conduct

At **Bradford Academy**, all users:

- Must use Academy IT systems according to the Acceptable Use Policy.
- Need to understand the consequences of misuse or accessing inappropriate materials.
- Should report abuse, misuse, or access to inappropriate materials and know how to do so.
- Must adopt good online safety practices outside the Academy, as the policy covers actions related to their membership.
- Should know and understand policies on mobile phones, digital cameras, handheld devices, image use, and online bullying.

Staff:

- Must read and follow the Academy's online safety policy, including the use of mobile phones and handheld devices.

Students/Pupils:

- Should understand research skills, avoid plagiarism, and uphold copyright regulations.

Parents/Carers:

- Should understand the rules of appropriate use and the sanctions for misuse.

Incident Management

At **Bradford Academy**:

- The online safety policy is strictly monitored and enforced with appropriate sanctions, though positive user behaviour often makes sanctions unnecessary.
- The community is encouraged to report issues confidently, knowing they will be handled quickly and sensitively through escalation processes.
- Support is sought from external agencies (e.g., local authority, Bradford Learning Network, UK Safer Internet Centre) as needed.
- Online safety incidents are monitored, reported, and used to improve policy and practice. Records are reviewed and reported to senior leaders and Governors.
- Parents/carers are informed of online safety incidents involving their children.
- The Police are contacted if staff or pupils receive particularly disturbing or illegal online communication.

External Agencies

Bradford Academy liaises with and accesses support from:

- West Yorkshire Police
- Social Services
- Bradford Learning Network
- Children's Social Care
- Third party support providers
- Bradford Council

4. Managing the IT and Computing Infrastructure

Internet Access, Security, and Filtering

Bradford Academy:

- Uses filtered & secure broadband.
- Employs filtering policies to block inappropriate sites (e.g., pornography, race hatred, illegal content). Changes to filtering are logged and managed by approved staff.
- Utilizes real-time monitoring of IT use, with safeguarding risks sent to Safeguarding Officers.
- Applies user-level filtering to tailor access based on student age/stage.
- Maintains network health with endpoint protection, scanning all EXE files.
- Uses DfE/LA approved systems for secure data transfer and encrypted devices for off-site access.
- Blocks chat rooms and social networking sites, except for educational networks or approved platforms.
- Unblocks external social networking sites for specific educational purposes.
- Blocks access to music download or shopping sites, except for approved educational purposes.
- Partners with our Internet Provider to address system concerns and ensure robust protection.

Supervision and Usage:

- Supervises pupil use vigilantly and employs common-sense strategies in flexible access areas.
- Requires all staff and students to adhere to the acceptable use agreement and report concerns.
- Ensures pupils publish only within secure environments (e.g., Learning Platforms).
- Requires staff to preview websites and encourages the use of the Learning Gateway/VLE for directing students to appropriate sites.
- Uses child-friendly search engines for open Internet searches.
- Monitors Internet use and requires reporting of filtering system failures to IT Support.
- Educates users on appropriate use rules and sanctions through meetings and programs.
- Provides advice on reporting offensive materials and refers suspected illegal content to authorities.

Network Management (User Access, Backup)

Bradford Academy:

- Uses individual, audited logins for all users and guest accounts for temporary access.

- Employs classroom management software for classroom management and monitoring.
- Ensures up-to-date Information Systems Directory/Manager policies.
- Conforms to UK data protection requirements for data storage and EU directives for online data storage.
- Requires staff to read and sign the online safety policy before gaining access.
- Provides unique log-in credentials for pupils and staff.
- Prohibits logging in as another user and restricts pupil access to staff log-ins.
- Sets up network document areas for saving and accessing work.
- Requires users to log off when finished or leaving a computer unattended.
- Requests computers be switched off at the end of the day to reduce power consumption.
- Blocks access to non-educational music/media download or shopping sites.
- Ensures loaned computers are used for professional responsibilities and significant personal use is reported.
- Maintains equipment to health and safety standards.
- Configures network access based on staff roles and encrypts remote access.
- Restricts external agency network access to professional needs through approved systems.
- Provides access to content and resources via learning platforms.
- Manages daily backups and has a disaster recovery system for critical data.
- Encrypts pupil and personal data sent over the Internet.
- Follows ISP advice on security and configures firewalls and routers to prevent unauthorized use.
- Secures the wireless network to industry standards.
- Regularly reviews IT systems for health, safety, and security.

Password Policy

Bradford Academy:

- Requires staff and pupils to keep passwords private and not share them.
- Provides unique usernames and passwords for system access.

Email

Bradford Academy:

- Provides professional email accounts for staff and requires personal email use through separate accounts.
- Maintains and updates email accounts.
- Reports illegal activity-related messages to authorities.
- Uses technologies to protect against spam, phishing, and viruses.

Pupils:

- Use Microsoft Outlook Web Access with appropriate restrictions.

- Are taught email safety and etiquette, including not sharing email addresses, writing clear messages, and reporting uncomfortable or offensive emails.

Staff:

- Use Academy email systems for professional purposes only.
- Are aware of email rules and sanctions for inappropriate use.
- Do not transfer personal data externally without encryption.

Bradford Academy Website

Bradford Academy:

- Ensures website content accuracy and quality.
- Restricts information uploading to authorized staff.
- Complies with DfE publication guidelines.
- Credits sources and avoids using pupils' names in images.
- Uses password protection for approved blogs or wikis.

Learning Platform

Bradford Academy:

- Shares information uploading responsibilities among staff.
- Restricts access to photographs and videos to the Academy community.
- Requires pupils to upload and publish within approved systems.

Social Networking

Bradford Academy:

- Prohibits teachers from using personal social network spaces for student use.
- Maintains preferred systems for social networking in line with the communications policy.

Staff:

- Do not reference students, parents, or staff in social media.
- Avoid online discussions about Academy community members.
- Ensure personal opinions are not attributed to the Academy.
- Regularly check social media security settings.

CCTV

Bradford Academy:

- Uses CCTV for site surveillance and safety.

- Does not reveal recordings without permission, except to the Police.
- Uses lesson recording equipment for teaching practice sharing.
- Follows best practices and complies with surveillance regulations.

5. Data Security: Management Information System Access and Data Transfer

Strategic and Operational Practices

At **Bradford Academy**:

- The Information Systems Director serves as the Senior Information Risk Officer (SIRO).
- Staff are informed on how to report data protection incidents.
- All staff are DBS checked, with records held centrally in our MIS.
- All stakeholders (staff, governors, pupils, parents) must read the Acceptable Use Agreement, outlining responsibilities for data security, passwords, and access.
- Government guidelines are followed for data transfer to professionals in Local Authority or partner services.
- Protect and Restricted material must be encrypted if removed from the Academy. Remote access solutions are provided to avoid data removal.
- Staff setting up usernames and passwords for email and network access follow approved security processes.
- Annual housekeeping is conducted to review, remove, and destroy unnecessary digital materials.

Technical Solutions

- Staff have secure network areas for sensitive documents or photographs.
- Staff must log out of systems when leaving their computer.
- Encryption for flash drives for off-site sensitive information.
- Personal data sent off-site must be securely encrypted; paper-based data must be transferred securely.
- Multi-Factor Authentication is required for accessing certain applications outside the Academy.
- The School2School system is used for secure CTF pupil data file transfers.
- Protected and Restricted written material is stored in lockable cabinets in a secure room.
- Servers are located in a locked server room managed by DBS-checked staff.
- Backup systems are used for disaster recovery on network servers and other critical systems.
- Equipment disposal complies with the WEEE directive, using approved disposal companies and obtaining secure deletion certificates.
- Portable equipment used for protected data follows the same disposal procedure.
- Sensitive paper-based information, CD-ROMs, and Mifare cards are shredded.

Software Purchases

All software purchases (including free software) must be assessed by the IT Team and Data Protection Officer before submission to the Finance Team.

IT Team:

- Assesses software compatibility with internal and cloud systems, including Microsoft365 and SSO.
- Evaluates security implications, including known bugs and infrastructure risks.

Data Protection Officer:

- Assesses data requirements and determines if a Data Protection Impact Assessment (DPIA) is necessary.
- Assists in completing the DPIA for software requiring Sensitive Personal Data (e.g., Medical, SEN, Financial data).

If serious failings are found by the IT Team or DPO, the software should not be purchased. Unauthorized purchases may result in unusable software.

6. Equipment and Digital Content

Laptops and Storage Devices

- All staff hard drives (HDD) must be encrypted before use outside the school. Other storage devices should also be encrypted.
- Emails are not encrypted and should not be used to transfer personal data. Use encrypted zip files or the School2School website for confidential information. Passwords for encrypted files should be given to the IT Director.

Personal Mobile Phones and Mobile Devices

- Mobile phones seen with learners will be confiscated and kept at reception until the end of the school day. Parents/carers will be notified.
 - First offence: Student collects the phone at the end of the day.
 - More than 3 offences: Parents/carers must collect the phone, and a behaviour point is issued.
- Post-16 learners can use mobile phones in designated study areas.
- Staff may use phones during breaks and PPA.
- Recording, taking, and sharing images, video, and audio on mobile phones is prohibited unless explicitly authorized by the Principal.
- The Academy reserves the right to search mobile devices on premises if there is suspicion of undesirable material.
- Parents/students should contact each other through the Academy office during the school day.
- Mobile phones brought to the Academy are at the owner's risk. The Academy is not responsible for loss, theft, or damage.
- Mobile phones are not permitted in certain areas (e.g., changing rooms, toilets).
- Mobile phones should not be used during lessons unless part of an approved activity.
- Bluetooth should be off and not used to send files.
- No images or videos should be taken without prior consent.

Students' Use of Personal Devices

- Breaching the policy results in confiscation. Devices are returned to students on the first offence or to parents/carers as per policy.
- Phones are not allowed in exams. Possession during an exam may lead to withdrawal from exams.
- Students needing to contact parents/carers should use Academy phones.
- Students should only share phone numbers with trusted individuals and are taught safe use of devices.

Staff Use of Personal Devices

- Permitted images/files taken in the Academy must be downloaded and deleted by the next working day.

- Staff should not use personal phones to contact students or families unless in exceptional circumstances.
- Staff will be issued Academy phones for required contact. In emergencies, staff should use their own device with hidden numbers.
- Personal devices should be off or on silent during teaching periods unless permitted by senior leadership.
- Breaching the policy may result in disciplinary action.

Digital Images and Video

- Parental permission is obtained for using digital images/videos of children.
- Pupils are not identified in online materials, and full names are not used in credits.
- Staff Acceptable Use Policy including clauses on using personal equipment for taking pictures.
- Access to social networking sites is blocked/filtered unless for educational purposes.
- Pupils are taught about image manipulation and safe publishing practices.
- Pupils are advised to maintain privacy settings and not post images/videos of others without permission.

Asset Disposal

- Hardware and software inventories are maintained.
- Redundant equipment is disposed of through authorised agencies with written receipts and secure deletion guarantees.
- Storage media is forensically wiped or physically destroyed if failed.
- Disposal conforms to WEEE regulations.