BRADFORD ACADEMY TRUST

Responsibility | Respect | Resilience

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

Information Security Policy

Approved by:	RMC	**Date:** December 2025
Last reviewed on:	December 2025	
Next review due by:	December 2026	
Related Documents		
Guidance	General Information Security policy	
Author	**Data Protection Team**	

TABLE OF CONTENTS

1 INTRODUCTION AND SCOPE

The Information Security Policy outlines Bradford Academy's organisational security processes and standards. It is based on the sixth principle of the UK GDPR, which states that organisations must protect personal data against unauthorised loss by implementing appropriate technical and organisational measures.

To ensure we meet our legal obligations, personal data should be protected by the security model known as the 'CIA' triad. These are three key elements of information security:

- Confidentiality – only authorised people should have access to information.
- Integrity – information should be accurate and trustworthy.
- Availability – authorised people should have access to the information and systems they need to carry out their job.

This policy, including its appendices, applies to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for or on our behalf. Individuals found to knowingly or recklessly infringe this policy may face disciplinary action.

The Information Security Policy applies to all personal data, whether paper or electronic. It should be read alongside the other policies within our information governance policy framework.

2 ROLES AND RESPONSIBILITIES

Overall responsibility for ensuring that we meet the statutory requirements of any legislation lies with the Board of Governors or Trustees. The following roles will have day-to-day responsibility for information security management and providing the necessary assurance to the Board.

2.1 SENIOR INFORMATION RISK OFFICER (SIRO)

The SIRO is responsible for overseeing the implementation of this policy and ensuring that effective information security practices are in place across the organisation. The SIRO is also responsible for risk management and will ensure that staff are appropriately trained in information security, supported by the DPT and IAOs. In our organisation, this role lies with the Executive Principal.

2.2 DATA PROTECTION TEAM (DPT)

The DPT take on the duties of what is also commonly referred as 'Single Point of Contact (SPOC)'. The DPT is responsible for overseeing the implementation of this policy and ensuring that effective information security practices are in place across the organisation. The DPT is also responsible for risk management and will ensure that staff are appropriately trained in information security, supported by the IAOs. This includes providing guidance on information security practices and promoting compliance with this policy to protect personal data in line with the CIA triad. In our organisation, this role lies with the IT Director, Data Manager and Finance Director.

2.3 INFORMATION ASSET OWNER (IAO)

IAOs will be responsible for the security and maintenance of their assigned information assets and for ensuring that other staff members use the information safely and responsibly.

2.4 ALL STAFF

All staff, including governors or trustees, contractors, agents and representatives, volunteers, and temporary staff working for or on our behalf, will be responsible for information security in accordance with this policy.

3 ACCESS CONTROL

We will maintain control over access to the personal data that we process. These controls will differ depending on the format of the data and the role of the individual accessing the information. We will maintain a record detailing which individuals have routine access to which information systems in our IAR.

3.1 MANUAL FILING SYSTEMS

Access to manual filing systems (i.e., non-electronic systems) will be controlled by a key or PIN locking mechanism. When not in use, all files containing personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe.

Keys to storage areas will be held securely and managed by the Site Director. Access will only be given to staff members who require it to carry out legitimate business functions.

3.2 ELECTRONIC SYSTEMS

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to perform legitimate functions. Wherever possible, multi-factor authentication will be implemented across all critical electronic systems.

Individuals will be required to comply with our password standards. Accounts will be immediately suspended when a staff leaves our employment or where it has been otherwise requested to protect data confidentiality.

Systems will be provisioned with Single Sign On (SSO) where possible to prevent the use of simple passwords across different systems. Where a system requires a manually entered password, the password will be unique to ensure that if one system is compromised, it does not lead to access to other systems. Users should never leave a live session unattended while logged in.

3.3 PASSWORD MANAGERS

Where possible, the IT department and those with access to systems containing sensitive information will utilise password management software which is used to store passwords securely. This practice helps to prevent insecure workarounds such as adopting insecure passwords that are easier to remember, re-using passwords, or making minor variations to previous passwords.

3.4 SOFTWARE AND SYSTEMS AUDIT LOGS

We will ensure that all critical software and systems have built-in audit logs wherever possible so that they can monitor what users have accessed and what changes have been made. Although this is not a preventative measure, it supports the integrity of the data and acts as a deterrent for individuals seeking to access records without authorisation.

3.5 DATA SHIELDING

We will not allow our workforce to access the personal data of family members or close friends wherever possible. Users should declare whether they know any family members or friends registered with us upon employment. When such an interest is raised, we will review access controls for relevant paper and electronic files to ensure that only appropriate access is granted.

Users who knowingly fail to declare family and friends registered with us may face disciplinary proceedings and be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

3.6 EXTERNAL ACCESS

Occasionally, we may need to allow individuals outside our workforce access to our systems. This could be for audit purposes, to fulfil an inspection, when using agency staff, or because of a partnership arrangement with another educational establishment. The SIRO or DPT, or if unavailable, an appropriately senior staff member, will authorise instances of third parties having access to systems.

We will maintain a record on our IAR detailing what access has been given to whom and the authorising individual.

4 PHYSICAL SECURITY

We will maintain high physical security standards to prevent unauthorised access to personal data. We will maintain the following controls:

4.1 CLEAR DESK POLICY

Staff members will not leave data subject to UK GDPR legislation or other data that could otherwise compromise the Academy in any ways left unattended on desks or workspaces. Lockable storage units or cabinets will be used to secure such data when not in use.

4.2 PORTABLE STORAGE DEVICES

Bradford Academy staff should not routinely use portable storage devices such as USB memory sticks and external hard drives to store or transfer pupil, staff, or business-related information. Where it is necessary to do so the device needs to be securely encrypted and the data should not be subsequently transferred to third party systems.

4.3 BUILDING ACCESS

External doors to the premises will be locked when the building is not occupied. Only authorised individuals will be key holders for the building. The Site Director is responsible for authorising the distribution of keys and maintaining an up-to-date log of all key holders. The Academy employs access cards and magnetic locks to regulate both external and internal entry to the premises. Upon an employee's departure from the Academy, their access cards are promptly revoked. In the event that an access card is lost or stolen, staff members must notify the Site Director or Facilities Team immediately so that access can be suspended without delay.

External contractors or visitors may need an access card in certain situations. Records will document which cards have been issued, recipients, and the dates of issue. The log will be reviewed at regular intervals, and any unaccounted-for cards will be suspended.

4.4 VISITOR CONTROL

Visitors must sign in, providing their name, organisation, car registration (if applicable), and the person they are visiting. Additional information may be requested for emergency support. Access is tracked electronically. All visitors must read and sign a visitor agreement, be escorted on site, and are not allowed in restricted areas without supervision unless appropriate checks have been carried out.

4.5 SECURE DISPOSAL

We will ensure that all personal data is securely disposed of per our Records Management Policy and retention policy. Hard copy information will be securely destroyed by a cross-shredder or a confidential

waste provider. Electronically held information will be deleted automatically, with retention periods built into systems, wherever possible. Otherwise, manual review and deletion will take place annually at a minimum.

Redundant computer equipment will be securely wiped and disposed of following the Waste Electrical and Electronic Equipment (WEEE) Regulations. Where personal devices are being disposed of, the user must ensure that they have complied with this policy. School-related data should be removed and stored appropriately within the appropriate systems before disposal.

5 ENVIRONMENTAL SECURITY

We must maintain high standards of physical security to protect personal data against unauthorised access and environmental and natural hazards such as power loss, fire, and floods. It is accepted that these hazards may be beyond our control, but we will implement the following mitigating controls:

5.1 BACK-UPS

We will regularly back up our electronic data and systems and conduct tests to ensure they can be restored correctly. These backups will be held in a different location from the main server room, off-site by an external provider, or using appropriate cloud storage. A data processing agreement will govern this arrangement. Should an environmental or natural hazard compromise our electronic systems, we will be able to reinstate the data from the backup with minimal disruption or data loss.

5.2 FIRE-PROOF CABINETS

We will provide lockable data storage cabinets that can withstand short fire exposure. This will protect any business-critical paper records held in cabinets from minor fires on the building premises.

5.3 SECURITY ALARM SYSTEMS

We will ensure that appropriate security systems are in place to alert individuals in the event of a fire or intruder. Extra measures, such as fire doors, will be implemented in areas where paper records or critical electronic equipment are held to provide extra security in an emergency event.

Emergency contact details will be in place and shared with the necessary services to ensure we can be contacted out of hours in the event of alarm system triggers.

6 SYSTEMS AND CYBER SECURITY

We will protect against hazards to our IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect our ability to operate and could potentially endanger the safety of our pupils and workforce.

We will implement security controls to mitigate risks to our digital devices and online locations, such as the cloud. All use of devices to access our network or systems must be authorised. We will ensure that, at minimum, devices have up-to-date security systems and encrypted storage, and that all software patches are installed as soon as they are released. All users will ensure these criteria are met for their personal devices wishing to access Academy resources, seeking specialist advice if required.

6.1 SYSTEM CONFIGURATION AND SOFTWARE DOWNLOAD RESTRICTIONS

We will restrict users from downloading third-party apps and software onto our devices. Users must request authorisation from the IT Support Department, who will vet the software to confirm that it does not pose a security risk. A list of trusted and deployed software will be retained.

All device configurations are managed centrally, and administrative access is restricted exclusively to IT Support personnel. No users outside the IT Support department will have the ability to modify settings that could affect device security or performance.

6.2 FIREWALLS AND ANTI-VIRUS SOFTWARE

We will ensure that firewall infrastructure is deployed, and anti-virus software is installed on electronic devices where possible. We will also update security releases as soon as possible to address any weaknesses. We will review our firewall setup and anti-virus software annually to assess if they remain fit for purpose. In addition, the Academy will deploy an Endpoint Detection and Response solution on all endpoints such as laptops, desktops, and servers to detect and respond to threats in real-time. EDR technology uses data analysis and correlation to identify malicious activities and provides tools for incident response, like isolating infected devices to contain attacks and prevent the spread of malware or ransomware

6.3 SHARED STORAGE

We will maintain shared storage on our servers with restricted areas only authorised users can access. The IT Support department will be responsible for providing users with access. Information held within shared storage will remain subject to our retention policy.

6.4 CLOUD STORAGE

We will liaise with our IT provider before utilising cloud storage. We will only use providers who can meet our security needs and demonstrate assurance with the National Cyber Security Centre (NCSC) Cloud Security Principles.

6.5 MALICIOUS SOFTWARE AND FRAUD

To avoid our systems being compromised fraudulently by email, users will consider the source of emails before clicking on any links or opening attachments. Users will check with our IT Support if they are unsure about the validity of an email, and must immediately inform IT Support if they have clicked on a suspicious link.

We will ensure staff receive adequate training to identify phishing, spear phishing, whaling emails, and other malicious threats. Staff identified as at higher risk of being targets for this type of fraud will receive regular training to combat the risk of social engineering and other types of fraud. Additional protections will be implemented to automatically check any links for potential fraud and any emails sent from external sources will be clearly marked accordingly.

The IT department will also run periodic phishing simulations involving staff, any users that are identified as falling victim to these emails will be sent additional training that will require completion.

Users will be safeguarding from running malicious software by limiting the execution of particular file types and scripts on Academy owned devices. All software will be checked by multiple anti-virus programmes before deployment regardless of source.

7 COMMUNICATIONS SECURITY

The transmission of personal data is a key Academy need and, when operated securely, benefits us and students alike. However, data transmission is susceptible to unauthorised or malicious loss or corruption. We will implement the following transmission security controls to mitigate these risks:

7.1 SENDING PERSONAL DATA BY POST

We will use Royal Mail's standard postal service when sending personal data, excluding special category data, by post. Individuals will double-check addresses before sending and ensure that the sending envelope does not contain data not intended for the data subject.

7.2 SENDING SPECIAL CATEGORY DATA BY POST

We will restrict sending special category data by post wherever possible. Where necessary, we will use a signed-for postal service to track delivery. Individuals will double-check addresses before sending and ensure that the sending envelope does not contain data not intended for the data subject. If the information is particularly sensitive, a colleague will double-check the contents.

7.3 SENDING PERSONAL DATA BY EMAIL

We will only email personal and special category data using secure email transmission methods, such as end-to-end encryption and encryption protocols. Individuals will double-check the recipient's email address to ensure that the email is being sent to the intended individual(s). The use of autocomplete for recipient email addresses will be discouraged.When it would not be appropriate for recipients to know each other's email addresses, , the Blind Carbon Copy (BCC) function will be used where no alternative option exists.

Where attachments are involved, particularly, but not limited to Microsoft Excel. The file will be reviewed to ensure that only data related to the recipient is included. This includes checking for hidden columns, rows or sheets. Where special category data is involved, the contents of files should be checked by a colleague unless the sender is confident that only applicable data is included.

Staff must not use personal email accounts to access or transmit pupil, staff, or business data. Only business-issued email accounts should be used.

7.4 EXCEPTIONAL CIRCUMSTANCES

In exceptional circumstances, we may wish to hand deliver or use a direct courier to ensure the safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too large for usual transmission methods.

8 REMOTE WORKING

8.1 PERSONAL DEVICES

Any electronic device not provided by us and used to access or process personal or business data will be classed as a personal device. The use of personal devices must be authorised and meet the requirements set out in this policy.

Personal devices must be limited to the individual user and not a shared resource, e.g., a family device. Users must only access the information they are entitled to in order to fulfil their role. To prevent

unauthorised access, devices must include appropriate security and access controls, such as password and/or PIN protection.

All staff members must use multi-factor authentication to access Academy resources. Students will be required to implement multi-factor authentication if their accounts are identified as being at risk or if access is initiated from outside the United Kingdom.

Pupil, staff, and business data must not be downloaded or stored on personal devices. All such information is to remain within designated systems to maintain security, ensure accessibility for authorised personnel, and facilitate proper management throughout its lifecycle, including secure disposal in accordance with our retention schedule. Printing personal data using home printers is strictly prohibited.

The IT department reserves the right to implement restrictions that may limit the downloading, forwarding, copying, or printing of Academy data at their discretion.

8.2 SECURITY AND CONFIDENTIALITY

Users must ensure that electronic equipment or paper documents containing personal data are kept secure and never left unsupervised. Any paper documents requiring disposal must be securely destroyed using a cross-cut shredder or returned to our premises for confidential waste disposal.

Individuals must not work in areas where others may view, hear, or copy personal data. Users must always be mindful of their surroundings and ensure measures are in place to prevent loss or unauthorised access to information.

When remote working, only trusted Wi-Fi connections will be used, with appropriate anti-virus and firewalls installed to safeguard against malicious intrusion. Unsecured network connections, including public Wi-Fi or hot spots, must not be used, and devices must be configured to prevent automatic connection to unknown networks.

Users will be mindful of any applications (apps) installed on personal devices that could be used to access pupil, staff, or business data. The user must seek reassurance that any risks associated with apps monitoring the device's use are being effectively managed.

Lost or Stolen Academy devices must be reported immediately to the IT Department.

8.3 AUTHORISED ACCESS

Access to business systems and cloud storage on personal devices is only permitted where authorised. Access should not be attempted when a user leaves employment or the working relationship ceases. Attempts to do so will be treated as a data breach and investigated as such. Under Section 170 of the Data Protection Act 2018, knowingly accessing data you are not entitled to is a criminal offence.

Any exemptions to the above access can only be authorised by the SIRO or DPT and will only be given where there is a clear business need and following a full risk assessment.

9 DATA BREACHES

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to personal data. The severity of breaches can vary from minor to very severe, however all breaches will be treated seriously. Appropriate measures will be in place to ensure continuous improvement of information security practice, reducing the risk of minor breaches or near-miss incidents from turning into high-risk breaches.

Where a data breach is likely to result in a high risk to the rights and freedoms of the data subject(s), Article 33 of the UK GDPR requires data controllers to report these to the Information Commissioner's Office (ICO), and sometimes the affected data subject(s), within 72 hours of discovery.

All actual and suspected breaches of security or confidentiality, including near misses, will be recorded and investigated in accordance with the Data Breach Procedure set out in Appendix One.

10 BUSINESS CONTINUITY

We will have an IT Incident Response Plan which includes a risk-based business continuity matrix to enable us to continue critical business in the event of an IT based incident. This plan will include the process to follow, emergency contacts, and Academy Critical priorities. We will ensure staff are aware of these arrangements and can access the plan easily.

We will have a process for testing, assessing, and evaluating the effectiveness of our information security measures. This may include vulnerability scanning and penetration testing.

We will obtain appropriate insurance, including cybersecurity coverage, to cover the costs of a serious cyber event. We will also ensure that all staff complete cybersecurity training in accordance with the insurance policy requirements.

APPENDIX ONE – DATA BREACH PROCEDURE

IMMEDIATE ACTIONS (WITHIN 24 HOURS)

If any member of the workforce becomes aware of an actual data breach or an information security event (a 'near-miss'), they must report it to the Data Protection Team (DPT) within 24 hours. If the DPT are unavailable, the SIRO, IT Director, Data Manager or nominated deputy must start the investigation process.

If the breach has the potential to be serious or cause wide-reaching detriment to data subjects, then the Data Protection Officer service must also be contacted within this 24-hour period.

If appropriate, the DPT or the individual who discovered the breach will make every effort to retrieve the information and ensure recipients do not retain a copy of the disclosed data. This may involve asking email recipients to delete data from their inboxes and recycle bins or collecting paper records in person. Measures to retrieve disclosed information will be dependent on the level of risk. Written confirmation should be sought from the recipient to confirm that the information is no longer held.

ASSIGNING AN INVESTIGATION (WITHIN 48 HOURS)

The DPT will begin to complete a data breach form and assess the data protection risks using a risk matrix to determine the severity rating. If the breach is assessed to be moderate or above, the DPT will inform the SIRO.

The DPO service should be sent a copy of the data breach form and the risk matrix to ensure the breach has been assessed appropriately and to recommend further measures to mitigate or reduce the risk.

REPORTING TO THE ICO AND/OR DATA SUBJECTS (WITHIN 72 HOURS)

Where the breach is assessed as high or very high risk, it should be reported to the ICO within 72 hours.

The DPT, in liaison with the SIRO and DPO service, will agree on whether the incident will be reported to the ICO and whether any data subjects should be informed. The DPO will prepare the ICO report and, once approved by the SIRO, submit it and liaise with the ICO until the matter is concluded.

The decision to notify data subjects will depend on the level of risk and any detriment or harm that could result from the disclosure. We will also consider what is in the best interests of the data subjects when making the decision. The DPT will be responsible for liaising with data subjects where it has been deemed appropriate to inform them.

INVESTIGATING AND CONCLUDING INCIDENTS

The DPT will ensure that all investigations have been completed, all potential information risks have been identified, and remedial actions have been implemented. Where necessary, the DPT in liaison with the SIRO should review the completed data breach form and action plan to ensure the breach was handled appropriately and actions completed.

All actual data breaches and near-misses must be recorded on the data protection platform under the 'Incidents and Breaches' log, along with the risk rating, actions taken, and investigation outcome. Any lessons learned should be shared and used to improve working practices.

APPENDIX TWO – WORKFORCE IT ACCEPTABLE USE POLICY

1 INTRODUCTION AND SCOPE

IT is an integral part of the way our Academy works, and is a critical resource for staff, pupils, governors, volunteers, contractors and visitors. It supports teaching and learning, and the pastoral and administrative functions of the Academy.

The IT resources and facilities our Academy use could also pose risks to data protection, online safety and safeguarding. This document governs the use of Bradford Academy devices, the IT network and provided cloud-based systems, including when authorised to use personal devices.

This policy aims to:

- Set guidelines and rules on the use of Bradford Academy IT resources for staff, volunteers, contractors, visitors, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the Bradford Academy community engage with each other online
- Support the Academy's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to Bradford Academy through the misuse, or attempted misuse, of IT systems
- Support the Academy in teaching pupils safe and effective internet and IT use

The document governs our workforce's use of the corporate network and cloud-based systems, including when authorised to use personal devices. It should be read in conjunction with the Academy's Data Protection policy, Records Management policy and relevant privacy notices.

Breaches of this policy will be dealt with by the Academy in accordance with the disciplinary procedures outlined in the terms and conditions of employment. The appropriate level of sanctions will be applied as determined by the nature of the reported misuse.

2 UNACCEPTABLE USAGE

Unacceptable use of computers, devices and network resources may be summarised as:

- Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate
- Threatening, intimidating or harassing employees and students including any message that could constitute bullying or harassment, e.g. on the grounds of sex, race, disability, religion or belief, sexual orientation or age
- Breaching the Academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Using obscene, profane or abusive language

- Using language that could be calculated to incite hatred against any ethnic, religious or other minority group
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights
- Defamation (genuine scholarly criticism is permitted)
- Unsolicited advertising often referred to as "spamming"
- Sending emails that purport to come from an individual other than the person actually sending the message
- Attempts to break into or damage computer systems or data held therein
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised
- Connecting or permitting the connection any device to the Academy's IT network without approval from authorised personnel, excluding the designated BYOD visitor network
- Using the IT facilities to conduct personal commercial business or trading
- Causing a data breach by accessing, modifying, or sharing data (including personal data) without proper authorisation or beyond a user's permitted access.

This is not an exhaustive list. The Academy reserves the right to amend this list at any time. The Executive Principal or any other relevant member of staff will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Academy's IT facilities.

Members of the Academy workforce should consider the spirit of the Academy Ethos when working on Academy IT systems. Any conduct which may discredit or harm the Academy, its staff or the IT facilities or can otherwise be considered intentionally unethical is deemed unacceptable.

3 PRIVACY AND MONITORING

Bradford Academy reserves the right to monitor activity, email, telephone and any other electronically-mediated communications, whether stored or in transit, in line with relevant legislation. All users acknowledge that their use of of Academy IT facilities or equipment may be accessed or viewed by the Academy.

Reasons for such monitoring include the need to:

- Ensure appropriate use of our assets and resources, in compliance with our rules and policies.
- Promote wellbeing and early intervention in high-risk incidents.
- Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes)

- Investigate or detect unauthorised use of Academy telecommunications systems and ensure compliance with this policy or other Academy policies
- Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems)
- Prevent breach of the law or investigate a suspected breach of the law, the Academy policies or contracts
- Monitor standards and ensure effective quality control
- Meet our statutory safeguarding obligations

Monitoring may involve:

- Examining the number and frequency of emails
- Viewing sent or received emails from a particular mailbox
- Viewing sent or received electronic chat-based messages e.g. Microsoft Teams conversations
- Examining logs of IT facility usage
- Monitoring the amount of time spent on the Internet; Internet sites visited, search history and information downloaded
- Automated screen capture of activity deemed a potential safeguarding concern
- Telephone call activity

Where abuse is suspected a more detailed investigation involving further monitoring and examination of stored data may be undertaken.

Where disclosure of information is requested by the police, (or another law enforcement authority) the request should be directed to the Data Protection Team.

Members of the Academy workforce that have access to personal data, (as defined under the Data Protection Act 2018) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

The Academy reserves the right to access workforce members' Academy email accounts and documents following the termination of employment or contract for operational purposes and to ensure the continued delivery of services. All actions will be conducted in compliance with UK GDPR and relevant data protection legislation.

4 EMAIL, INSTANT MESSAGING, AND INTERNET USE

We provide users with email accounts, Teams instant messaging (IM) functionality, and Internet access to assist with performing their duties where applicable. For the benefit of doubt, Teams instant messages and emails are classed as electronic communications in this policy.

Users should use these accounts and systems in accordance with our Information Security Policy. In particular, users should not:

- Click on links from untrusted or unverified sources
- Use insecure email transmission methods when sending personal data

- Sign up for marketing material that could jeopardise our IT network
- Send emails to an excessively large number of recipients unnecessarily

4.1 Personal use

Whilst email accounts, Teams instant messaging, and the Internet should primarily be used for Academy functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Use must not tarnish our reputation or infringe on business functions
- Electronic communications sent to and from corporate accounts are our property
- We may monitor the use of accounts and systems and access any personal messages and browsing history contained within
- Electronic communications sent to or from their account may be disclosed under Freedom of Information and/or Data Protection Legislation
- We reserve the right to cleanse email and Teams instant messaging accounts at regular intervals, which could result in personal communications being erased from the corporate network
- We reserve the right to suspend access to accounts and systems anytime.

4.2 Other business use

Users are not permitted to use emails, Teams instant messaging or the Internet to carry out their own business or the business of others. This includes, but is not limited to, work for political organisations, not-for-profit organisations, and private enterprises. The Executive Principal may lift this restriction on a case-by-case basis.

4.3 Shared email accounts

Users may be permitted to send and receive emails from shared and/or generic email accounts. These shared email accounts must not be used in a personal capacity, where appropriate users should ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of shared email accounts could lead to the suspension of a user's email rights or access to the shared email account.

The IT Support department will be responsible for allowing access to shared email accounts. All email traffic to and from individual and shared accounts may be monitored.

5 ACCOUNT ACCESS AND SECURITY

The Academy's IT Support Department manages access to the Academy's IT facilities and materials for staff, students and visitors. This includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes, online resources or files

All users will be provided with unique login/account information and passwords that they must use when accessing the Academy's IT facilities.

Staff, governors and other users with access to privileged information will require Multi-Factor Authentication when connecting to Academy resources from outside the Academy's network.

Users who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Support Department. All requests will be reviewed and permission sought from the Information Asset Owner of the specific resource.

All users of the Academy's IT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or the governing body who disclose account or password information may face disciplinary action. Visitors, contractors or volunteers who disclose account or password information may have their access rights revoked.

The Academy does not mandate periodic password changes, however, should you suspect your password has been compromised then you must change your password immediately.

Users should not use a private VPN when connecting to Academy resources.

Users will not attempt to download any software onto Academy devices outside of the 'Company Portal' application. Doing so can present a virus risk and/or breach of software license requirements.

6 SOCIAL MEDIA AND PRIVATE MESSAGING APPS

We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. However, we also recognise that social media poses a data protection risk due to its open nature and capacity to broadcast to many people quickly. As such it is imperative that the following guidance is adhered to.

6.1 COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

Social media should never be used in a way that breaches any of our other policies. If a social media post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

- breach our IT policies and procedures.
- breach our Disciplinary Policy or procedures.
- breach our Anti-bullying Policy.
- breach our Equal Opportunities Policy.
- breach our Data Protection obligations (for example, never disclose personal information about a colleague or student online)
- breach any other laws or regulatory requirements.

Workforce members who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Workforce members should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

Workforce members must make themselves aware of and act in accordance with their duties under the DfE statutory guidance Keeping Children Safe as these relate to:

- their own on-line activity
- the on-line activity of learners and other colleagues and
- information of which they become aware on-line including their duties relating to Children Missing from Education, Child Sexual Exploitation, FGM and Preventing Radicalisation (Prevent).

6.2 CORPORATE ACCOUNTS

We may have social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about our business activities. Authorised users will be given the usernames and passwords to these accounts, which must not be disclosed to any other user within or external to the organisation. The Data and Marketing Manager will be responsible for allowing access to corporate social media accounts. The creation of social media accounts representing the Academy is strictly prohibited without authorisation of the Data and Marketing Manager.

Corporate social media accounts must not be used to disseminate personal data in an open forum or by direct message. Doing so would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

- Tarnish our reputation
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs
- Be construed as sexually explicit
- Be construed as political beliefs or commentary.

6.3 PERSONAL ACCOUNTS

We understand that many users will use or have access to personal social media accounts. Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy. Staff should never be on social media when teaching or supervising children.

In addition:

- You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.
- You must not use social media to defame or disparage us, our staff, learners, parents/carers or any third party; to harass, bully or unlawfully discriminate against learners, parents/carers, staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- You must not express opinions on our behalf via social media, unless expressly authorised to do so by the leadership team. You may be required to undergo training in order to obtain such authorisation.
- You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property.
- Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and learners both within and outside of school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for 'cyber-bullying', for example, or identity theft.
- Staff should not make 'friends' or follow learners (or recent learners) of the school because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any pupils (the potential for colleagues at the Academy to be compromised in terms of content and open to accusations makes the risk not worth taking). Staff should keep all communications with pupils transparent and professional, should not send messages or post comments on learners' social media and should only use the school's systems for communications
- Colleagues at the Academy are also strongly advised not to be friends with learners at other schools (on or off-line) as this is likely to make them vulnerable to allegations and may be open to investigation by the Academy or police. Where a colleague is considering not following this advice, they are advised to discuss the matter and the implications with the Executive Principal, a member of Senior Leadership or the designated safeguarding leaders. Staff should also carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality.
- New employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

- You must not share any personal information with any student (including personal contact details, personal website addresses/social networking site details) and ensure good safeguarding practice.
- Caution is advised when inviting work colleagues to be "friends" in personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships if too much personal information is known in the workplace.
- You must not post or share photographs or videos of learners under any circumstances unless:
    - You have a personal connection with the learner that is entirely unrelated to your role at Bradford Academy (e.g. you are the learner's parent or family member), **and**
    - The content is unrelated to school activities, events, or settings.

  For example, a parent may share a photo of their child receiving exam results, provided the image does not include other learners or staff, and is not taken during an official school event.
- Any misuse of social media should be reported to HR

6.4 PRIVATE MESSAGING APPS

Social messaging apps such as WhatsApp, Facebook Messenger, Signal etc. must not be used for communicating any school business. Information held in non-corporate communication channels may be subject to FOIA if it relates to official business.

7 TELEPHONE AND VIDEO CONFERENCING USE

We provide users access to telephone and video conferencing services to assist with communication and performing their duties.

7.1 PERSONAL USE

Whilst telephone and video conferencing services should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Usage must not tarnish our reputation or infringe on business functions
- We may monitor and access call history and recordings
- We reserve the right to suspend telephone and video conferencing usage at any time
- Telephone calls, video conference recordings, or transcripts may be disclosed under the Freedom of Information and/or Data Protection Legislation.
- Excessive usage or the use that incurs significant expenses outside of expected use are not permitted.

7.2 Inappropriate Use

We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

7.3 Other Business Use

Users are not permitted to use these services to carry out their own business or the business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.

APPENDIX THREE - PUPIL ACCEPTABLE USE AGREEMENT - SECONDARY PHASE

INTRODUCTION

Most of us use digital technologies daily, both within and outside school. These technologies can help your education and development by promoting creativity, curiosity, and engagement with the wider world. With an awareness of the risks involved, you should have safe access to these digital technologies and the opportunities they provide.

This Acceptable Use Agreement outlines what is expected of pupils when using the Academy's network and related technologies to maintain the safety and security of the systems and other users.

This applies to the Academy's computers, mobile devices such as laptops and tablets, personal devices such as mobile phones, and any activity that uses computer networks, such as the school's Wi-Fi.

INTERNET, APPS, AND EMAIL USE

The Academy provides you with an email account and allows you to use specified apps and the Internet for educational purposes.

Whilst your Academy email account and devices should primarily be used for educational purposes, you may use them in a personal capacity so long as:

- It does not negatively impact the learning environment for other pupils and staff
- It does not damage the reputation of the Academy
- You understand that Bradford Academy monitors your use of its network and systems, and can access your email account and Internet browsing history.

The school does not permit you to use emails, apps or the Internet in any way that could be insulting, disruptive, or offensive to someone else. Material not allowed includes, but is not limited to:

- Sexually explicit messages, images, cartoons, jokes, or movie files
- Profanity, obscenity, slander, or libel
- Ethnic, religious, political, or racial slurs
- Any content that could be seen as bullying or belittling of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs

You are also not permitted to use the Internet in a way that could negatively affect others' usage. This means not downloading software, the excessive streaming or downloading of media files such as music or films, or playing online games.

You must also be aware of copyright restrictions when using the Internet. You are not permitted to use materials in ways that would infringe intellectual property laws, including copyright. This means you should be careful when reusing online materials and content.

Security

You will take care to use accounts and systems with information security in mind. In particular, you will:

- Not click on links from untrusted or unverified sources in emails or on web pages
- Keep your passwords unique, private, and do not share them with others
- Log out when you are finished or lock your account when away from the device
- Not sign up for marketing material that could jeopardise the school's IT network
- Not send very large files without authorisation from a member of staff
- Not attempt to download any apps or software onto the Academy's devices or network
- Not attempt to connect unauthorised devices to the Academy's network

Monitoring

In order to support and protect pupils and staff, we monitor your use of the computer network, including:

- Checking and reviewing all email traffic to and from your accounts
- Monitoring your Internet and browsing activity
- Using software that blocks banned content, monitors device activity, and notifies the school of any inappropriate use or safeguarding concerns
- Monitoring of all Bradford Academy devices regardless of location

Social media use

Using social media during school time is not permitted.

You should not use social media in a way which violates the privacy or dignity of other users, including staff, pupils and other members of the wider community

Remote learning

If you are learning remotely, you may engage in more online activities than usual and be provided with accounts for more services.

All of the expectations above apply when you are accessing your school accounts from home, such as when completing home learning or in the event of remote classrooms. When learning from home, you should also:

- Not leave drinks or food near your schoolwork, computer or devices to prevent damage to work or equipment
- Only using appropriate methods to contact school staff, such as using designated school email accounts
- Remember that the Academy's behaviour policy and classroom expectations still apply to virtual classrooms
- Avoid using VPNs when connecting to school resources, this may result in your account being flagged as 'at risk' and result in additional security measures applying to your account.

For access or certain services, multi-factor authentication may be required, this is to safeguard the security of the Academy's IT network and services. For more information speak to IT Support.

Safe use of online services

In addition to the safe applications the Academy provides for your educational use, pupils should take care when using online services independently. Some online services are paid for, and others are free at the point of use but are funded by advertisements. These are used at the individual's request and at the user's risk.

Online services may include:

- Apps
- Games
- Social media
- Streaming services
- Anything that offers goods and services

Pupils should be particularly mindful of protecting their personal information and safety when using the Internet, both within and outside school. Before using any online service, pupils should consider whether the service:

- Is age appropriate
- Uses child-friendly language and methods of communication
- Has high privacy settings in place by default, e.g. private rather than public profiles
- Has privacy and safety options such as blocking and reporting

- Allows you to set the user age
- Has location tracking switched off by default

These considerations help to protect and promote your safety and best interests.

Use of Artificial Intelligence (AI):

AI tools and technologies can be valuable resources for enhancing learning and providing guidance. However, it is important to use these tools responsibly and ethically.

AI should be used to support and guide pupils in their learning process, not to replace the effort and hard work required to understand and master new concepts.

Pupils are encouraged to use AI for:

- Research and gathering information.
- Receiving feedback on their work.
- Enhancing creativity and problem-solving skills.

Pupils should not use AI to:

- Complete assignments or exams on their behalf.
- Plagiarise or copy content without proper attribution.
- Bypass the learning process by relying solely on AI-generated answers.

Consequences of inappropriate use

Inappropriate use may result in sanctions in line with the Academy's behaviour policy. If you misuse the computer network and related devices, the Academy may:

- Remove your access to the Internet or network account
- Temporarily ban you from using school equipment
- Confiscate your personal device(s)
- Contact your parent or guardian
- Take further action, as appropriate
- Wilful or intentional damage to ICT facilities may result in your parent(s) / carer(s) being invoiced for the cost of replacement of the facilities.

Responsible rules for ICT

The Responsible Rules for ICT offer a concise overview of key areas. These rules are displayed to pupils in classrooms and upon accessing IT facilities, ensuring they are informed regularly of essential online safety practices and the standards expected of them:

10 rules for responsible ICT use:

These rules will help keep everyone safe and help us to be fair to others. By using Bradford Academy IT devices you accept the following rules

- I will not look at other people's files without their permission and will only delete my own files
- I will only do schoolwork during lessons
- I will keep my login and password secret
- I will not keep inappropriate files on the school network or in my user account
- The messages I send and the things I upload will only be polite and sensible
- I will only communicate with people I know and/or those my teacher has approved
- If I am unhappy with a message received, or come across any content which appears to be inappropriate, I will not respond to it and will report it to a member of staff
- I will treat the ICT equipment with respect and will not cause damage to it
- I will not download or upload anything which is offensive, illegal or is copyrighted
- I will use the Internet and AI tools responsibly and ethically and only as tools to support my learning. I will not use them to replace the hard work required to understand and master new concepts.

AGREEMENT

When accessing Bradford Academy IT equipment, networks and facilities, you agree to abide by these rules.

I have read and understand the above apply when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment outside of school in a way related to schoolwork, e.g. communicating with other pupils or teachers, accessing school email, website, etc.

Pupil name:

Pupil signature:

Date:

APPENDIX FOUR - PUPIL ACCEPTABLE USE AGREEMENT - PRIMARY PHASE

Information for Parents and Guardians

Digital technologies have become integral to children's and young people's lives, both within and outside school. These technologies are powerful tools that open up new opportunities for everyone. They can stimulate discussion, promote creativity, and raise awareness, which promotes effective learning. Young people should always be entitled to safe digital and Internet access.

This Acceptable Use Agreement is intended to ensure that:

- pupils will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use
- our digital systems are protected from accidental or deliberate misuse that could put the security of our systems and users at risk
- parents and guardians are aware of the importance of e-safety and are involved in the education and guidance of young people regarding online behaviour.

Pupil Acceptable Use Agreement

I understand that I must use digital technology responsibly by doing the following:

- I will only use computers or tablets with permission from a teacher or a suitable adult.
- I will only use applications that a teacher or a suitable adult has allowed me to use.
- I will take care of the computer, tablet, and other equipment.
- I will ask for help from a teacher or a suitable adult if I am unsure what to do or think I have done something wrong.
- I will tell a teacher or a suitable adult if I see something that upsets me on the screen.
- I will not use Artificial Intelligence to complete work for me or to copy other people’s work and pretend it is my own

When accessing Bradford Academy IT equipment, you agree to follow these rules.

I have read and understand the above and agree to follow these rules when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment outside of school in a way related to schoolwork, e.g. communicating with other pupils or teachers, accessing school email, website, etc.

If I break the rules, I might not be allowed to use a computer or tablet for schoolwork.

Pupil name:

Class:

Pupil signature:

Date:

Parent or Guardian Permission

As the parent or guardian of the named pupil, I give permission for my child to access the Internet and digital systems at Bradford Academy.

I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the Internet, both in and out of school.

I understand that Bradford Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that my child is safe when using the Internet and digital systems.

I understand that my child's activity on digital systems will be monitored and that Bradford Academy will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to use the Internet and digital technologies safely at home and will inform Bradford Academy if I have concerns about my child's e-safety.

I understand that if my child wilfully and purposefully damages IT equipment, the school reserves the right to invoice me for the cost of the replacement of the equipment.

Parent or guardian name:

Parent or guardian signature:

Date: