Information Security Policy

Our Ambition: To be the highest performing MAT in the country

Our Mission: To improve the communities we serve for the better

Written by	C Braithwaite
Date for Review	November 2021
Approving Body	The Strategic Development Committee
Signed Chair of Trustees	

Vision:

Challenging educational orthodoxies so that every child makes good progress in core subjects;
all teachers are committed to personal improvement and fulfil their responsibilities;
all children receive a broad and balanced curriculum;
all academies strive to be outstanding.

1. Introduction

1.1 Information is one of the Trusts most important assets. Failure to ensure adequate security and protection of information held by the Academy or Trust may lead to legal action against the Academy and/or the individual responsible for the breach. Such legal action could include an investigation by the Information Commissioner's Office ("ICO") who can impose significant financial penalties and/or a claim for damages for breach of the General Data Protection Regulation and the Data Protection Act 2018 (together the "Data Protection Legislation").

1.2 In addition to the possibility of legal action being taken against the Academy or Trust, if the information held by the Academy or Trust is not kept safe, confidence in the Academy and the Trust by pupils, parents/carers, volunteers, the Board of Trustees, members of staff and the public at large could be irreparably damaged.

1.3 Keeping information secure yet available to those that need it often presents a difficult challenge. This policy strives to achieve a sensible balance of securing the information held by The Forge Trust and our academies while making it accessible to those who need the information. The trust and our academies will always however favour security.

2. Definitions

2.1 *The Trust"* means The Forge Trust.

2.2 "*Data Protection Legislation"* means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.3 *"Data"* means Personal Data and Special Category Personal Data as defined by the *Data Protection Legislation*, and confidential and sensitive information held by the Trust.

2.4 "*Personal Data*" any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.5 *"Special Category Personal Data*" means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

2.6 "*Processing*" means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

2.7 *"Data Controller"* is the organisation which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing

3. Summary

3.1 Much of the information held by the Trust is confidential and sensitive in nature. Therefore, it is necessary for all information systems to have appropriate protection against

adverse events (accidental or malicious) which may put at risk the activities of the Academy or protection of the information held.

3.2 The Academy has a responsibility to maintain:

- **Confidentiality** – access to Data must be confined to those with specific authority to view the Data in question;
- **Integrity** – information should be complete and accurate. All systems, assets and applicable networks must operate correctly and according to any designated specification;
- **Availability** – information must be available and delivered to the right person at the time when it is needed and in accordance with the relevant statutory provisions.

3.3 The Academy must minimise the risk of data security breaches and any person connected to or acting on behalf of the Academy must meet the minimum requirements as set by the Academy/Trust for connecting to any network operated by or on behalf of the Academy.

3.4 It is important that members of staff, trustees or anyone else acting on behalf or with the authority of the academy or trust:

- Are aware of how and under what circumstances they are permitted to access Personal Data held by or on behalf of the Academy;
- Are aware of who they are allowed to share Personal Data and other information with and how it can and should be shared;
- Reports any Information Security incidents/breaches including phishing emails[1] to the Data Protection Officer in respect of information held by the Academy.
- A Data Breach report must be filled out and passed to the DPO after initial reporting of a breach.
- Ensures Data is stored and handled securely and in accordance with this and the other information governance and IT Policies;
- Does not ignore, turn off or otherwise bypass any Information Security controls put in place by the academy;
- Does not send, distribute or otherwise divulge Data unless permitted to do so.

  The sending or distribution of any Data should only be done in accordance with the applicable statutory provisions, this policy and any other applicable policy of the academy;
- Data must only be sent by secure methods and, all data sent externally shall be encrypted or sent with the appropriate level of sensitivity.

4. Policy Statement

4.1 It is essential that the academy's information systems and data networks are adequately protected from events which may compromise the information held or the carrying on of academy business and to this end the academy is committed to developing and maintaining an information systems structure which has an appropriate level of security.

4.2 The academy will maintain the security and confidentiality of data held by it, its information security systems and relevant applications and networks for which it is directly responsible by:

- Ensuring appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services;
- Ensuring that it is aware of, and complies with, the relevant legislation as described in this and the other information governance and IT Policies;
- Describing the principles of Information Security to Members of Staff, pupils, trustees and volunteers and explaining how they will be implemented by the academy;
- Creating and maintaining a level of awareness of the need for information security to be an integral part of the conducting of Academy business and ensuring that everyone understands their individual and collective responsibilities in this respect;
- Protecting Data and other information held by and/or on behalf of the Academy.

4.3 To ensure a consistent approach to Information Security, the controls set out at sections 7 and 8 of this policy will apply.

5. Use of Client and Personal Devices

5.2 Client Devices used for, or in connection with, Academy business must not be left unattended in plain sight at any time, including whilst at home or travelling, and must be protected against loss, damage, misuse or unauthorised access. When not in use, Personal Devices must be stored in a secure location and should never be stored in vehicles, even if locked.

5.3 Client Devices/ Personal Devices used for, or in connection with, Academy business must not be used to access, view or process Personal Data or Special Category Personal Data in a manner that allows Persons other than the Authorised User to view the Data.

5.5 Client Devices/ Personal Devices used for, or in connection with, Academy business must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated.

5.6 Client Devices/ Personal Devices used to store Personal Data or Special Category Personal Data must be encrypted/ protected by two factor authentication

5.7 Client Devices issued to a Member of Staff for or in connection with, Academy/ Trust business by the Academy/ Trust must not be used by employees of another organisation or other users where a data risk is presented.

5.8 If a Client Device/Personal Device used for, or in connection with Academy business it lost or stolen, the loss/theft should be reported to Data Protection Officer and IT Support Team as soon as possible and in any event within 24 hours of the loss/theft occurring. Where possible the Client Device should be remotely accessed and the information erased.

6. Removable Media must not be used to data for which the Trust or Academy is responsible for.

7. Securing Information

7.1 Physical Access Controls

- A nominated member of the Academy/ Trust will be responsible for ensuring the Information Security of all Information Assets held by or on behalf of the Academy. The nominated person will also have and maintain an Information Asset Register which should record all Information Assets held by the Academy;
- A copy of the Information Asset register will be filed with the Data Protection Officer at the Trust each year;
- The Academy will ensure that only authorised individuals are allowed access to restricted filing cabinets containing Personal Data or Special Category Personal Data or information systems where there is an identifiable need for access. Keys to filing cabinets will be carefully monitored and controlled.
- Access to Personal Data and/or restricted files will be monitored by the Academies nominated person to ensure authorised access to relevant information and to prevent unauthorised access to Personal Data or Special Category Personal Data;
- Where an unidentified person or any other person without authorisation accesses secure files, the individual is to be challenged as to their identity and the purpose for which they are in the restricted area. If the unauthorised individual has no legitimate reason to access the restricted files, this information is to be logged as an Information Security Breach and the Data Protection Officer should be consulted as to whether the matter requires reporting to the ICO;
- External doors and windows must be locked at the end of each day;
- Equipment that serves multiple users must be capable of identifying and verifying the identity of each authorised user;
- Devices or equipment capable of displaying output upon multi-user displays or presentation equipment, including but not limited to, Projectors, Interactive Whiteboards, televisions, video walls, remote computer sessions and desktops, or any other form of presentation equipment, must not be used to access, view or process Data in a manner that allows Persons other than the Authorised User to view the Data.
- Members of staff of the Academy/Trust with access to and use of Data must maintain a clear desk and clear screen policy to reduce the risk of unauthorised access to Information Assets such as papers, media and information processing facilities;
- Academy wireless systems should be secured to industry standard Enterprise security level/appropriate standards suitable for educational use;
- Data recorded on paper must be kept locked away in a safe, cabinet or other form of secure furniture when not in use;
- Personal Data and Special Category Personal Data, confidential and sensitive information about the Academy whether stored electronically or on paper must be kept locked away in a secure room or in a safe, cabinet or other form of secure furniture when not in use;
- Documents containing Data must not be left unsecured, unattended at mail points or on printers, photocopiers, scanners or fax machines and must be removed immediately when received.

7.2 Password and Access Control

- Access to Data stored electronically must be controlled through the use of a Strong Password;

- Access to Authorised User accounts must be controlled, as a minimum, through the use of a password, which must not be less than 6 ASCII characters in length.
- Wherein, a system or service, provides alternative authentication methods, including but not limited to, facial or biometric recognition, the alternative authentication method must be in additional to a password;
- Members of Staff must ensure that they have a Strong Password for all Authorised User accounts and the same password not re-used across different types of system;

- Authorised Users are responsible for keeping their assigned password(s) secure and must ensure their password(s) is neither disclosed to, nor used by, anyone else under any circumstances;

- Use of another person's username or password without consent for legitimate purpose will constitute an Information Security Breach and must be reported in accordance with the procedures set out in this policy or any other relevant policy from time to time in force (where it is necessary to access a colleges device for legitimate trust purposes the original user must change their password following this);

- Authorised Users are responsible for ensuring that all Academy and/or Client/ Personal Devices used to access Data or other confidential information, are logged off, switched off or otherwise controlled by a Strong Password when unattended or not in use, at all times

- Authorised Users with access to the Academy network or a Client Device which is used for, or in connection with Academy business is responsible for any actions carried out under their username and password.

- Where available, Members of Staff using critical systems or accessing Personal or Special Category Personal Data should use Two-Factor Authentication.

7.3 Cloud Computing

- Only cloud computing networks or services, including Social Media commissioned by the Academy, or expressly authorised by the Data Protection Officer, may be used to store and send information concerning or relating to Academy business. The use of personal cloud storage solutions (Skydrive, Onedrive Personal, iCloud, G-Drive etc.) for the transfer of Academy information is expressly forbidden.

- Personal Data, Special Category Personal, confidential and sensitive information, whether on the Academy/ Trust network or a Client Device must not be stored on a cloud computing network or service not commissioned by the Academy, or expressly authorised by the Data Protection Officer.

- If Data or other information concerning or relating to Academy/ Trust business is to be stored in or on a cloud network, the Academy will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA.

- If the Academy receives notification that Data in respect of Academy business has been corrupted, lost or otherwise compromised while stored on a cloud network, the Academy should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information;
- Any corruption, loss or compromise of information held on a cloud network should be recorded in the risk register and if appropriate reported via the mandatory reporting procedure set out at section 9 of this Policy.

7.4 Leaving the Academy/Contract Termination

- Upon leaving the Academy, Members of Staff must return/transfer, in a useable format, all equipment and information, including Data to the Academy, on or before the agree leaving date (e.g. last day of employment) to their Line Manager, or other Academy representative if their Line Manager is not available. This includes, but is not limited to:
- All information, including data, used or stored as part of the role, both physical and electronic;
- All information, including files, documents and emails, including any Data, stored within individual Cloud Service accounts;
- Client Devices loaned by the Academy, including PIN numbers, usernames or passwords required to reuse or reset the devices;
- Access control, PIN, tokens and ID Cards;
- Keys and PIN numbers used to access physical locations.
- After leaving Members of Staff may not attempt to access or use any Academy information, including any Data.

8. Storing and Transportation of Non-Electronic Data

8.1 Data can be vulnerable to loss, unauthorised access, misuse or corruption when being physically transported either personally by Member of Staff of the Academy or when sending Data via the postal service or couriers;

8.2 Special controls should be adopted where necessary to protect Data from unauthorised disclosure or modification and may include:

- Ensuring the packaging is sufficient to protect the contents from any physical damage likely to arise in transit;
- Delivering by hand records containing Personal Data, where appropriate;
- Sending Data via secure post such as Royal Mail recorded or signed for delivery or special delivery or as otherwise agreed with the Data Subject;
- Records containing Special Category Personal Data shall not be delivered by hand unless absolutely necessary. In which case the following should occur:
- Documents transported in vehicles should be hidden away or placed in boot where possible, and the vehicle locked.
- Documents should never be left unattended even in a locked vehicle.

8.3 Consideration should be given to the necessity of transporting or moving Data or other records as this increases the risk of Data loss.

9. Transportation/Transmission of Electronic Data

9.1 Personal Data, Special Category Personal, confidential and sensitive information sent or transmitted externally using an electronic systems or services must be secured

using a process that ensures the Data is encrypted and Users must carefully check the recipient's contact details before sending.

9.2 Data must only be sent or transmitted externally when authorised by job description, Trust policy, applicable legislation, or when specially authorised by the Data Protection Officer. The sending of Personal Data and Special Category Personal Data to personal cloud systems or services email accounts is expressly forbidden. Members of staff working remotely are required to access Data through the Trust's authorised systems and services.

9.3 Data must not be sent using any systems or services, including but not limited to, cloud platforms and social media providers or any other type system not owned by the Academy, including text messaging.

9.4 Personal Data and Special Category Personal Data must be sent to named Users only. Multi-User posting, sending or transmission, including, but not limited to, email lists, distribution groups, security groups, chat/team-based groups, forums, rooms, and channels is prohibited.

10. Information Security Incident Reporting and Management

10.1 The Academy will have and maintain a register where all Information Security incidents are logged. The form in Appendix 4, can be used as the basis for the Information Security incidents to the Data Protection Officer. = This log as a minimum should include:

- The nature of the breach;
- The number of Information Assets compromised;
- How the Information Asset(s) has/have been compromised;
- Whether any Special Category Personal Data was compromised;
- Whether the incident needs to be reported in accordance with the mandatory reporting section of this policy at paragraph 10.3 below.

10.4 Examples of an Information Security Breach include but are not limited to:

- Password(s) written down or stored, in an accessible, plain text or otherwise visible, manner to persons other than the Authorised User;
- Using another person's password;
- Divulging of a password;
- Making use of Personal Data for personal gain;
- Accessing Data for personal knowledge;
- Attempting to gain access under false pretences;
- Unauthorised release of Data;
- Knowingly entering inaccurate Data;
- Deleting Data prior to the retention period or any other period set out in the Retention, Disposal and Records Management policy expiring;
- Loss or misuse of Data;
- Malicious damage to equipment or Data;
- Changing permissions that allows access to, or sharing information (including Data) with, persons not authorised to access the information.

- Unauthorised removal of Data, Academy equipment or equipment used for or in connection with Academy business from Academy premises or another site authorised for the storage of such information or equipment
- Loss or theft of a Client Device used for or in connection with Academy and/or Trust purposes or any other device belonging to the Academy or Trust.

11 Business Continuity and Disaster Recovery Plans

11.1 Each Academy will develop a managed process to counteract the interruption of Academy business caused by major IT service failure. The Academy will ensure that business continuity and disaster recovery plans are produced for all IT systems and networks which store and/or Process Data.

11.2 The Academy will have procedures in place to maintain essential services in the event of an IT system failure.

- **12. Monitoring and Review**

12.1 This policy will be reviewed every 4 years or earlier if required and may be subject to change.