The Oak Trust

Information Security Policy

Oak Trust
Inspirational Learning & Leadership

Co**ntents**

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 or Trust 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 financial penalties.

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, Local Advisory Members, Trust Board Members, 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 Academy while making it accessible to those who need the information.

1.4. 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.

1.5. The Academy has a responsibility to maintain;

1.5.1. Confidentiality – access to Data must be confined to those with specific authority to view the Data in question;

1.5.2. Integrity – information should be complete and accurate. All systems, assets and applicable networks must operate correctly and according to any designated specification;

1.5.3. 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.

1.6. The Academy must minimise the risk of data security breaches and any person connected to or acting on behalf of the Academy must meet minimum requirements as set by the Academy/Trust for connecting to any network operated by or on behalf of the Academy. This can be found in Appendix 1

1.7. It is important that members of staff, Local Advisory Members, Trust Board Members, or anyone else acting on behalf or with the authority of the Academy;

1.7.1. Are aware of how and under what circumstances they are permitted to access Personal Data held by or on behalf of the Academy;

1.7.2. Is aware of who they are allowed to share Personal Data and other information with and how it can and should be shared;

1.7.3. Reports any Information Security incidents/breaches including phishing emails to the Data Protection Officer (DPO) in respect of information held by the Academy;

1.7.4. Ensures data is stored and handled securely and in accordance with this and the other information governance, data and IT policies;

1.7.5. Does not ignore, turn off or otherwise bypass any Information Security controls put in place by the Academy;

1.7.6. 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;

1.8. Data should only be sent by secure methods and, where necessary, should be encrypted.

2. Policy Statement

2.1. 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.

2.2. 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:

2.2.1. Ensuring reasonable controls are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services;

2.2.2. Ensuring that it is aware of, and complies with, the relevant legislation as described in this and other information governance, data and IT policies;

2.2.3. Describing the principles of Information Security to members of staff, pupils, Local Advisory Members and Trust Board Members and explaining how they will be implemented by the Academy;

2.2.4. Creating and maintaining a level of awareness of the need for information security to be an integral part of the conducing of Academy business and ensuring that everyone understands their individual and collective responsibilities in the respect;

2.2.5. Protecting Data and other information held by and/or on behalf of the Academy.

2.3. To ensure a consistent approach for Information Security, the controls sections 5 and 6 of this policy will apply.

3. Access

3.1 Access to all systems and services are controlled by user accounts and passwords.

3.2 The systems and services are owned by Academy and are made available to staff to enhance their professional activities including teaching, research, administration and management.

3.3 Any internet access for personal use must be in staff's own time, i.e. before the start of the school day, break and lunchtimes (unless on duty) and after school. This does not include 'free periods' as this is part of staff's working hours.

4. Use of Client Devices

4.1. Client Devices can either be Academy devices or personal devices not owned by the Academy.

4.2. Before using a Client Device for, or in connection with Academy Business, users must read and understand the Client Devices Statement round in Appendix 1.

4.3. Client Devices used for, or in connection with, Academy Business and in particular for the collection or storing of Personal Data and/or Sensitive Personal Data must be kept secure with Strong Passwords (see Definitions). If available with the device, an approved Secure Authentication Device may be used for Two-Factor Authentication to aid entering of the password;

4.4. Client Devices used for, or in connection with Academy business should be kept secure at all times and be protected against loss, damage, misuse or unauthorised access.

4.5. The use of Client Devices in public for, or in connection with Academy business should be kept to a minimum to reduce the risk on unauthorised access to Personal Data or Sensitive Personal Data.

4.6. Mobile Client Devices, including but not limited to, laptops, tablets, smartphones should not be used to store Personal Data or Sensitive Personal Data.

4.7. Client Devices used for, or in connection with Academy business where possible should have antivirus software installed and be updated with the manufacturer's software and other updates regularly when updates become available.

4.8. Personal data relating to Academy work must not be stored on a client device. You may not save copies or extracts of student or staff records or any related personal or sensitive information.

4.9. If a Client Device used for, or in connection with Academy business is lost or stolen, the loss/theft should be reported to the DPO 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.

4.10. Avoid accessing or transmitting sensitive/confidential data when connected to public and open wi-fi hot spots.

5. Remote access and working from home

5.1. Academy staff working at home or remotely are responsible for ensuring that all Academy information is kept confidential and secure to prevent access by a third party.

5.2. Even though Academy staff may be working in a different environment they are still required to adhere to all Information Security, Data Protection, Acceptable Use and all other relevant policies.

5.3. For home working you must ensure any paper information is locked away when not in use and is kept separate from valuables.

5.4. Information must not be left accessible to other people, e.g. family members, visitors, or members of the public.

5.5. Do not create or attempt to transfer Academy data to your client device.

5.6. Under no circumstances should personal or confidential information be emailed to a private non Academy email address

6. Removable media

6.1. Removable Media should not be used for the storing of Personal Data or Sensitive Personal Data unless the device is capable of, and has been encrypted. You must also seek permission from the DPO

7. Securing Information

7.1. Physical Access Controls

7.1.1. The Data Protection Officer will be responsible for ensuring the Information Security of all Information of all Information Assets held by or on behalf of the Academy. The DPO will also have and maintain an Information Asset register which should record all Information Assets held by the Academy;

7.1.2. The Academy will ensure that only authorised individuals are allowed access to restricted areas containing Personal Data or Sensitive Data or information systems where there is an identifiable need to access that area;

7.1.3. Access to Personal Data and/or restricted areas will be monitored by the Academies DPO to ensure authorised access to relevant information and to prevent unauthorised access to Personal Data or Sensitive Personal Data;

7.1.4. Where an unidentified person or any other person without authorisation to be in a restricted area is found, 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 be in the restricted area, this information is to be logged as an Information Security Breach.

7.1.5. External doors and windows must be locked at the end of each day;

7.1.6. Equipment that serves multiple users should be capable of identifying and verifying the identity of each authorised user;

7.1.7. Members of staff of the Academy with access to and use of Data will 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;

7.1.8. Client Devices, whether belonging to the Academy, or any Data Processor, that are used for, or in connection with Academy Business or Data Processing should be switched off or controlled by a Strong Password (see definitions) when unattended or not in use;
7.1.9. Academy wireless systems should be secured to industry standard Enterprise Security level/appropriate standards suitable for educational use;
7.1.10. Data recorded on paper should be kept locked away in a safe, cabinet or other form of secure furniture when not in use;
7.1.11. Confidential information about the Academy whether stored electronically or on paper should be kept locked away in a secure room or in a safe, cabinet or other form of secure furniture when not in use;
7.1.12. Documents containing Data should not be left unattended at mail points or on printers, photocopiers or scanners.
7.1.13. Where personal and/or sensitive information is being printed on shared printers' extreme care should be taken to ensure all documents are collected from the printer and that interruptions to printing due paper jams, empty trays etc. do not lead to sensitive documents being discovered by unauthorised users.
7.1.14. Waste paper containing confidential information must be placed in confidential waste sacks or security shredded.

7.2. Password and Access control
7.2.1. Members of staff of the Academy should not use the same password for multiple accounts, and they should not be written down.
7.2.2. Members of staff of the Academy should refer to the password advice at the back of this document.
7.2.3. Access to Data contained within or accessed from the Academy and/or Trust network(s) will be controlled and restricted to authorised users only;
7.2.4. Academy IT systems and services may allow control of the distribution of Data, such as file or sharing permissions. Members of staff are responsible for ensuring that any file or permissions do not allow unauthorised access or sharing of Data;
7.2.5. Members of staff of the Academy who have access to Data are responsible for keeping their own password secure and must ensure their password is neither disclosed to, nor used by, anyone else under any circumstances;
7.2.6. Members of staff of the Academy with access to the Academy network or a Client Device used for, or in connection with Academy business must only access the network or Client Device using their own username and password;
7.2.7. Use of another username and password 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 in force;
7.2.8. Each member of Staff of the Academy 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;
7.2.9. Where available, members of staff using critical systems or accessing Personal or Sensitive Personal Data should use Two-Factor Authentication.
7.2.10. Giving an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence

7.3. Leaving the Academy/Contract Termination
7.3.1. Upon leaving the Academy, members of staff must return/transfer, in a usable format, all equipment and information, including Data to the Academy, on or before the agreed leaving data (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;
7.3.2. All information, including data, used or stored as part of the role, both physical and electronic;
7.3.3. All information, including files, documents and emails, including any Data stored within individual Cloud Service accounts;
7.3.4. Client Devices loaned by the Academy, including PIN numbers, usernames or passwords required to reuse or reset the devices;
7.3.5. Any Removable Devices provided by the Academy;

7.3.6. Access control, PIN, tokens, ID Cards;
7.3.7. Keys and PIN numbers used to access physical locations.

7.4. After leaving member of staff may not attempt to access or use any Academy information, including any Data.

8. Storing and Transportation of Data

8.1. Data can be vulnerable to loss, unauthorised access, misuse or corruption when being physically transported either personally by members 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 modifications and may include;
8.2.1. Sending Sensitive Personal Data via secure post such as Royal Mail recorded or signed for delivery or special delivery or as otherwise agreed with the Data Subject;
8.2.2. Ensuring the packaging is sufficient to protect the contents from any physical damage likely to arise in transit;
8.2.3. Delivering by hand where convenient and/or appropriate;
8.2.4. Records containing Personal Data shall not be delivered by hand unless absolutely necessary. In which case the following should occur:
8.2.4.1.1. Documents transported in vehicles should be hidden away or locked in the boot where possible
8.2.4.2. Documents and Client Devices should not be left unattended even in a locked vehicle, especially overnight

8.3. If secure remote access is not possible, removal off site of Academy paper information assets containing personal data should only be done with authorisation from your line manager. Paper records should not be taken off site just because it is convenient to do so.

8.4. Prior to authorisation, a risk assessment based on the criticality of the hard copy information asset should be carried out.

8.5. Data sent or transmitted electronically must be secured using a process that ensures the Data is encrypted.

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

9. Information Security Incident Reporting and Management

9.1. The Academy will have and maintain a register where all Information Security incidents are logged. This log as a minimum should include:
9.1.1. The nature of the breach;
9.1.2. The number of Information Assets compromised;
9.1.3. How the information Asset(s) has/have been compromised;
9.1.4. Whether any Sensitive Personal Data was compromised;
9.1.5. Whether the incident needs to be reported in accordance with data protection legislation

9.2. Where there has been any breach the Data Protection Officer must be informed immediately so they can decide if an Information Security Breach has occurred and in order that consideration can be given to reporting the breach to the appropriate authorities;

9.3. Examples of an Information Security Breach include but are not limited to;
9.3.1. Password(s) written down and available by, on or next to a computer or Client Device used for or in connection with Academy business;

9.3.2. Using another person's password;
9.3.3. Divulging of a password;
9.3.4. Making use of Personal Data for personal gain;
9.3.5. Accessing Data for personal knowledge;
9.3.6. Attempting to gain access under false pretences;
9.3.7. Unauthorised release of Data;
9.3.8. Knowingly entering inaccurate Data;
9.3.9. Deleting Data prior to the retention period or any other period set out in the Retention and Destruction Policy expiring;
9.3.10. Loss or misuse of Data;
9.3.11. Malicious damage to equipment of Data;
9.3.12. Changing permissions that allows access to, or sharing information (including Data) with, persons not authorised to access the information;
9.3.13. 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;
9.3.14. 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.

10. Business Continuity and Disaster Recovery Plans

10.1. The 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.

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

9 Definitions

Data means Personal Data and Sensitive Personal Data

Data Subject means all living individuals about whom the Academy holds Data

Data Controller is the person or organisation which determines the purposes for, and the manner in which any Data is processed. The Oak Trust is the Data Controller in relation to this policy.

Data Processor means any person who or organisation which processes Data on behalf of the Data Controller including members of staff, suppliers and any third party whose work involves accessing or otherwise using Data held by the Academy

Information Asset means Data held by the Academy in any form. This Data may be held electronically, on paper, in files or transferred by post, courier or in person.

ICO means the Information Commissioner's Office

Information Security means the protection of data and information systems against unauthorised access to or modification of information, whether in electronic or manual storage, processing and against the denial of service to authorised users.

Information Security Breach means a breach which may be caused by a technical failure, unauthorised access to either the Academy's network or a Client Device used for Academy business by a third party, loss of the Academy's information and / or inappropriate actions of an individual or individuals which result in the compromise of information belonging to or held by the Academy

Client Device means laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment that could be used for the carrying out of Academy business or the processing or storing of information and that are either owned by the Academy or by the individual user.

Personal Data means any information relating to a living individual who can be identified, directly or in directly, from that data or from those data and other information which is in the possession or likely to come into the possession of the Data Controller

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

Sensitive Personal Data means information about a persons racial or ethnic origin, political opinions, religious or similar beliefs, trade union memberships, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

Appendix 1 Client Devices

The Oak Academy Trust recognises that its staff will use Client Devices to access work information and emails. This must be achieved with appropriate protection of the data that is held within the documents. Therefore all members of staff using Client Devices to access Academy documents and emails must adhere to the requirements below.

Client Devices include but are not limited to: mobile phones, tablets, laptops and PCs

Client Devices used for, or in connection with Academy business should be kept secure at all times and be protected against loss, damage, misuse or unauthorised access.

The use of Client Devices in public for, or in connection with Academy business should be kept to a minimum to reduce the risk of unauthorised access to Personal Data or Sensitive Personal Data.

Client Devices used for, or in connection with Academy business where possible should have antivirus software installed and be updated with the manufactures software and other updates regularly when updates become available.

Passwords

All Academy information, in particular Personal Data and / or Sensitive Personal Data must be kept secure with a strong password.

If the member of staff is the only person to access the Client Device that is being used for Academy work, then documents and web based programmes can be left open on the device as long as a strong password is used to access the device and the device is locked or shut down when left.

If a Client Device is used by numerous people then the documents / programmes / emails may not be kept open. They must be accessed through a strong password.

A strong password must be a minimum of 8 characters, does not use single common number sequences/dictionary words or easily accessible personal information. Strong passwords of less than 16 characters must include a combination of three of the following: lowercase and uppercase letters, numbers and symbols.

Lost or Stolen Client Devices

If a Client Device is lost or stolen and has access to Trust information on it, the following actions must be taken;

- Inform the Academy Data Protection Officer
- Immediately remotely access the programme and change the password, or
- Request the ICT Team reset your passwords

Appendix 2 Password Advice

Member of staff of the Academy Trust should ensure their passwords for are not accessible by others and follow the conditions below;

- Your password must be a minimum of 8 characters and must three of - uppercase character, lower case character, number, special characters
- Do not use the same password for multiple accounts, so that other systems are not put at risk if one is compromised
- Do not use dictionary works (two or three words strung together is fine)
- Passwords must not include proper names or any other personal information about the user that might be known by others
- Passwords must be kept confidential and are the responsibility of individual users. They must not be given to anyone else even for a short period of time. **Giving an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence**
- You can store your passwords in a reputable software password manager
- You must change your password immediately if you think anyone else may have found it out.