Information Security Policy

Version:	2.0
Approved by:	Finance Committee
Issue Date:	22 June 2021
Review Date:	June 2023

Table of Contents

Information Security

The availability of complete and accurate information is key to providing excellent services to students, parents, and staff. The Trust holds and processes a large amount of confidential and personal information on private individuals, employees, service partners, suppliers, and its own operation.

The Trust has a responsibility to protect its reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore, the confidentiality, integrity, availability and accountability of information need to be protected from harm in a way that is proportionate to the risks to the information.

This policy provides the overall framework to ensure that everyone plays their part in protecting student and staff information.

Scope

This policy applies equally to everyone who reads or processes Trust information, including:

- All staff, whether permanent, temporary or casual
- All governors and trustees
- All volunteers
- Contractors and consultants; and
- Partners and suppliers

Throughout this document the words "employee", "staff" and "user" are used to describe these groups of people.

The policy applies to all forms of information, including but not restricted to: text; pictures; photographs; maps; diagrams; video; audio; CCTV; and music, which is owned by, administered or controlled by the Trust including information which is:

- Spoken (face to face, by fixed line or mobile telephone, by two-way radio).
- Written (by hand or printed from a computer system – including when working on-site or remotely).
- Stored in structured manual filing systems.
- Transmitted by e-mail, fax, over the internet or via wireless technology.
- Stored and processed via computers, computer networks or mobile computing devices, including but not restricted to PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
- Stored on any type of removable computer media including, but not restricted to CDs, DVDs, tables, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices such as digital cameras, MP3 and MP4 players.

Purpose

1. To set out examples of good practice for the governance of personal data and information in all its forms, balancing the need to process and manage data set against risk of data breach.

2. To maintain and improve the security of our systems and the quality of our data by improving the data capability and awareness of our staff, students, and other users of the

Trust's data or computing and networking facilities and ensuring they are supported by appropriate tools and processes.

3. To ensure that 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

4. Both as an organisation and for individuals who process our data to ensure that we are aware of, and comply with, the relevant legislation as described in this and the other information governance and IT Policies

5. To describe the principles of Information Security to members of staff, pupils and other authorised persons and to explain how these will be implemented by the Trust;

6. To develop and maintain a level of awareness of the need for information security to be an integral part of the conducting of Trust business and ensuring that everyone understands their individual and collective responsibilities in this respect;

7. To protect personal data and other information held on our systems.

8. The impact of this policy will be to improve security and data management standards.

9. The terms 'personal data' and 'information' are used interchangeably in this policy, as are 'information security' and 'cybersecurity'.

This policy does not specifically address issues of privacy or personal data protection, although good data management and security are essential for compliance with data protection laws. Concerning privacy and data protection, the Data Protection Policy, Privacy Notices, E-Safety, CCTV and Whisteblowing policy precedence.

This policy will be regularly reviewed and updated to ensure it remains current.

Breaches of policy

Breaches of the policy will be investigated and may be met with disciplinary action up to and including termination of employment. The nature of the disciplinary measures will depend on a number of factors including the nature of the violation.

Any suspected breach should be reported immediately and the 'Breach and Non Compliance' procedure is to be followed (Appendix 1 in Data Protection Policy).

The legal framework

There are many laws and regulations governing how information is handled, including:

- Common law in relation to duties of confidentiality
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Children Act 1999
- Freedom of Information Act 2000

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988.
- Health and Safety at Work Act 1974.
- Theft Act 1978.
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- UK General Data Protection Regulations 2018 (UK GDPR)

Roles and responsibilities

All Information Users

- Comply with this policy and related processes, procedures, and guidelines.
- Comply with legal, statutory, regulatory, and contractual obligations related to information.
- Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to confidentiality, integrity, and availability.
- Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the Trust without proper authorisation.
- Report immediately to the CEO (in accordance with the Whistle Blowing Policy) all suspected violations of this and all other security policies; system intrusions; and any other security incident or weakness which might jeopardise the Trust's information or information systems.
- Read and act on any communications and training regarding information security, seeking clarification if these are not understood.
- Play an active role in protecting information in day-to-day work.

Trustees and SLT

- Approve this policy.
- Actively promote effective and appropriate information security using structured risk assessment in all future developments and by appropriate retrospective risk assessment of current processes and systems.
- Implement and promote Information Security to all staff within their service areas.
- Ensure that employees understand and abide by the Information Security policy and its associated policies, processes, procedures, guidelines and understand its impact.
- Assign owners to all information in their area of responsibility.
- Provide effective means by which all staff can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.

- Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
- Provide written authorisation for access to information.
- Ensure that communications regarding information security are cascaded effectively to all staff.
- Ensure that information security is an integral part of all departmental processes

Information Owners

- Use structured risk assessment to select security controls to protect their information.
- Monitor to ensure security controls continue to be effective and that information is being handled correctly.
- Report and act on security incidents and weaknesses relating to their information according to agreed incident management policies and processes.
- Manage the residual risks to their information.
- Prepare appropriate Business Continuity plans and contingency arrangements.

ICT Services e.g. ICT technician / network manager / etc)

- Be the custodian of electronic information in its care by implementing and administering technical security controls as appropriate.
- Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
- Assist the Trust to ensure all software is licensed and remove unlicensed software.
- Provide contingency arrangements for information systems.
- Provide appropriate protection from malicious software.
- Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
- Monitor and investigate technical security breaches.
- Provide technical support to enable compliance with this policy.

Data protection / Information security

Operating Within the Law

Information shall be always used legally, complying with UK and European law. All users, including employees, and agents of the Trust might be held personally responsible for any breach of the law.

All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the General Data Protection Regulation 2018. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed

to anyone inside or outside the Trust without proper authorisation.

Personal, confidential or sensitive information shall be protected appropriately at all times and in particular when removed from Trust premises either physically on paper or electronic storage devices, or when transmitted electronically outside the Trust.

Personal, confidential or sensitive information should not be included in the text of e-mails to be sent outside the Trust, or in files attached to them, unless these are securely encrypted or sent by secure network links.

Any request for information under the Freedom of Information Act 2000 (FOIA) shall be handled in accordance with the law and processed within 20 working days. Where an exemption to FOIA might apply, further advice shall be obtained from the Information Commissioner Office (ICO).

Information shall not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others. Electronic and non-electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity. Note; It is accepted that in some professional situations such information is required for business reasons.

The Trust shall only use licensed software on its computers, servers and all other devices. The Trust shall provide sufficient legally acquired software to meet all legitimate and agreed needs in a timely fashion.

Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of copyright

Controlling access to information

The requirements for confidentiality, integrity, availability and accountability shall be determined for all information, from creation to deletion.

Structured information security risk assessment shall be used to determine the appropriate security controls required to protect information, which are proportionate to the risks to the information and information systems. This risk assessment shall be undertaken as part of system and process development. The effort expended on risk assessment and the amount of formal documentation required shall be proportionate to the perceived risks to the information and the impact of a breach of its security.

Access to information shall be authorised by management, including sharing information with partners and other organisations. Briefings and formal acceptance of security policies are required before access is granted to certain information systems and facilities.

There shall be adequate separation of functions for tasks that are susceptible to fraudulent or other unauthorised activity.

Information users must not attempt to access information to which they do not have authority.

Information users shall always keep personal passwords confidential.

Agreements and contracts with external business partners and suppliers shall, where relevant, include the requirement to adhere to this policy.

All equipment, including network equipment, attached to the Trust's computer network shall be approved by the Headteacher before connection.

School equipment, facilities and information may only be used for the Trust's business purposes, unless written permission has been granted by the CEO and/or Headteacher. Trust equipment, facilities and information must never be used for personal gain or profit.

Non-Trust or personally owned equipment or storage devices may not be connected to the Trust's computer network or to any Trust-owned equipment, whether on the Trust network or not, without written permission from the CEO and/or Headteacher.

All information about the security arrangements for Trust computer and network systems and structured manual filing systems is confidential to the Trust and shall not be released to people who are not authorised to receive that information.

Protecting the availability of information

Business continuity plans shall include all aspects of the Trust's infrastructure, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems, information on mobile devices and storage, communications including telephone services, staffing requirements, transport facilities, electricity supply, office accommodation and maps.

Maintaining the integrity of information

- Users are not permitted to modify electronic or manual information storage or processing systems.
- Users shall use only the officially provided or approved facilities and systems to access Trust information.
- Users shall not interfere with the configuration of any computing device without approval.
- All devices that are subject to the threat of malicious software shall have anti-virus scanning software installed and regularly updated.
- Appropriate security patches will be applied to all devices that are subject to the threat of security vulnerabilities.

Processes and procedures

Personal Data

Personal data is any combination of data items that identified an individual and gives specific information about them, their families, or their circumstances. This includes names, contact details, gender, date of birth, behaviour and assessment records, medical records, criminal convictions, and ethnic origin, whether held electronically or on paper.

The Data Protection Act 2018 sets out 6 principles concerning personal data, requiring that it must:

- Be processed fairly and lawfully.

- Be processed for specified purposes.
- Be adequate, relevant and not excessive.
- Be accurate and up-to-date.
- Not be kept for longer than necessary for the specified purpose.
- Be processed in accordance with the rights of data subjects.
- Be protected by appropriate practical and organisational security.
- Not be transported (including electronically) outside the European Economic Area without ensuring protection for the data is at least as good as in the EEA.
- Parents and staff must be made aware that the information they give us may be recorded, may be shared in order to provide appropriate education and care, and may be used to support audit and other work to monitor the quality of education and care provided.

Keeping Records Secure

All records that include student / staff identifiable information will be stored securely in locked filing cabinets, password protected electronic databases or another form of restricted access storage when not in use.

Employees are expected to take appropriate measures to always ensure the security of personal data, including keeping records secure if visiting students in their homes.
Access to computer equipment should be restricted by closing windows and doors when the room / office is not in use. Computer screens should always be locked (Ctrl, Alt and Del) if being left switched on and unattended.

Access will be afforded on a "need to do" basis, and access of leavers removed promptly.
So far as is reasonably practicable only authorised persons will be admitted to rooms that contain servers or provide access to data.

Equipment and paper files must not be left on view in any public setting.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public.

Documents or files containing personal identifiable information should be saved onto a shared network, with appropriate security protection, and not onto the C: Drive.

All Trust-owned ICT equipment, including software, should be recorded and security marked.

Users must not make, distribute, or use unlicensed software or data on site.

Mobile devices (e.g. laptops, memory sticks, etc.) must be encrypted for all sensitive, personal or confidential data.

Passwords

- Passwords must not be shared with other members of staff under any circumstances.
- Passwords should not be written down and/or left on display or be easily accessible.

- Passwords should be "complex", comprising a combination of letters and numbers (preferably upper and lower case) and should be changed frequently.
- The "remember password" feature should never be used.
- Staff are encouraged to password protect any personal files, in particular those that contain potentially embarrassing information about an individual or an organisation.

Transfer / Sharing of Personal Data and/or Confidential Information

The Data Protection Act 2018 should be always considered when recording, sharing, deleting or withholding information.

Sensitive information must not be shared unless the person is authorised to receive it.
Any transfers of confidential information should be secure and the method risk assessed.
For electronic information transfers encrypted software should be used.

When information is requested by telephone it is important to:

- Ask the caller to confirm their name, job title, department and organisation and verify this by returning their call via their organisation's switchboard.
- Confirm the reason for the request.
- Be satisfied that disclosure of the requested information is justified.
- Place a record on the student / staff file noting the name of the person disclosing the information, the date and time of the disclosure, the reason for the disclosure, who authorised it (if applicable) and the recipient's details.

When sending personal or sensitive information by fax, the sender must:

- Check that the recipient fax machine is sited in a secure room and is not used by more than one department.
- Check that there is a designated person who will collect the fax.
- Telephone the recipient to advise that a confidential fax is being sent to them, confirm the fax number and request a receipt.

Ensure that a cover sheet is included with the fax and shows the name of the recipient and the following wording:

"The information contained in this fax is STRICTLY PRIVATE & CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error please notify the sender immediately. Thank you."

When sending personal or sensitive information by post:

- Check the name, department and address of the intended recipient.
- Use a robust envelope, clearly marked "PRIVATE & CONFIDENTIAL To be opened by the addressee only".

- Information to a service or department within the Local Authority should be sent using the internal post system.
- If the public post system is to be used a return address must be recorded on the outside of the envelope, and recorded delivery should be used if the information is highly sensitive.

Disposal of data / PCs / Laptops

All data, whether paper or electronic, must be disposed of properly and in accordance with the Trust's document retention and disposal schedule (found on the Trust website).

If a PC or laptop is to be given to another user, personal data should first be removed from it (e.g. student databases, free school meal information, etc).

PCs and laptops must be disposed of securely, through our current approved supplier list.
It is imperative that staff follow any guidelines issued when overwriting data. Sending information to a computer's recycle bin does not delete the data as such. It is therefore important to empty the recycle bin regularly.

Paper records containing personal data or confidential information must be shredded.

Monitoring

Use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure adherence to this policy.
- To detect and investigate unauthorised use of information.
- To maintain the effectiveness, integrity, and security of the computer network.
- To ensure that the law is not being contravened.
- To protect the services provided by the Trust to the public; and
- To protect the integrity and reputation of the Trust.

All monitoring shall be:

- Fair and proportionate to the risks of harm to the Trust's information and reputation.
- Undertaken to intrude on users' privacy only as much as is necessary.
- Carried out similarly regardless of whether the user is school-based or working remotely; and
- Carried out in accordance with legislative requirements.

Access to any records of usage will be stringently controlled.

Reporting information security breaches

In the event of loss or theft of computer equipment the CEO and/or Head Teacher must be informed at the earliest opportunity.

Security issues should be raised with the Head Teacher in the first instance. If this is not appropriate reference should be made to the Whistleblowing policy.

Security incidents and weaknesses can be reported to the following:

The Head Teacher
Trust CEO admin@oaktrust.org

Reports may be made by phone, face to face, or in writing.

Policy review

This policy shall be reviewed every two years.

This policy and its associated procedures and guidelines shall be updated according to:

- Internally generated changes (e.g. changes in organisation, technology, etc).
- Externally generated changes (e.g. changes in legislation, security threats, recommended best practice, etc).
- All users shall be informed of changes to this policy which affect them.