Information Security Policy

June 2022

Aims of the Policy

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 school'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 School.

6. To develop and maintain a level of awareness of the need for information security to be an integral part of the conducting of school 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 and Privacy Notices take precedence.

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

Relevant Legislation

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)

Personal Data

For purposes of this Policy, "Personal Data" means information that can identify an individual and is set out in the Data Protection Policy.

It is important to note that some data is more sensitive and must be treated with greater care and understanding about the basis to process this sensitive data that includes:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- trade-union membership
- genetic data, biometric data processed solely to identify a human being
- health-related data
- data concerning a person's sex life or sexual orientation

Implementation of this Policy

- Staff and authorised persons awareness will be managed through training and induction
- Regular testing of our IT and physical data safeguards
- Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the Personal data to which we have permitted them access; and requiring such third party service providers by contract to implement and maintain appropriate security measures
- Reviewing the scope of the security measures at least annually, or whenever there is a material change in our practices that may implicate the security or integrity of records containing personal data
- Conducting an annual training session for all relevant people who have access to Personal data on the elements of the policy, and keeping a record of attendees.

Storage of Information

The amount of personal data collected, and the time period for retention, should be limited to that amount reasonably necessary to accomplish our legitimate purposes, or necessary for the organisation to comply with other legal requirements, regulatory obligations and relevant advice from the Department for Education.

Systems to store data, including material from emails, will be in place to comply with our Record of Processing Activities. These may be physical or electronic/digital records.

Examples that set out more detail about good information management and security will be shared with staff and authorised persons. (see '20 Key Issues for Staff' in the Staff Training Section under GDPR on SharePoint) and Schedule 1 to this policy.

Physical Records — Records containing personal data (as defined above) must be stored appropriately, and records containing sensitive data should be stored in locked facilities, secure storage areas or locked cupboards or offices.

Electronic Records — To the extent technically feasible, the following security protocols must be implemented:

Secure user authentication protocols including:

- control of user IDs and other identifiers
- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices
- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect
- restricting access to active users and active user accounts only
- blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system

Secure access control measures that:

- restrict access to records and files containing personal data to those who need such information to perform their job duties; and
- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls

Encryption of the following:

- all transmitted records and files containing personal data that will travel across public networks, and encryption of all data containing personal data to be transmitted wirelessly
- all personal data stored on laptops or other portable devices
- reasonable monitoring of systems, for unauthorised use of or access to personal data;
- For files containing personal data on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal data
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

Access to Information

Access to records containing personal data shall be restricted to current employees or approved persons who are reasonably required to know such information in order to support the school's objectives.

Records containing personal data shall only be removed from the site with specific authorisation from a relevant member of SLT or as part of an employee's job description.

Staff and approved persons who have access to personal data will logoff their computers when not in use for an extended period of time.

During short periods of inactivity, these staff and approved persons will either lock their computers at the operating system level or ensure that no unauthorised person can gain access - this is of particular importance for computers or devise in classrooms or teaching areas if the device or computer is left unattended at any point.

Visitors to the site where personal data is stored shall not be permitted to visit any area of the premises that contains personal data unless they are escorted by a school employee. Employees are encouraged to report any suspicious or unauthorized use of personal data.

Transmission of Information

To the extent technically feasible, all records and files containing personal data which are transmitted across public networks or wirelessly must be encrypted or secured.

Staff and authorised persons are prohibited from keeping open files containing sensitive personal data on their desks or in their work or teaching areas when these are unattended by a member of staff or authorised person.

At the end of the school day, all files and other records containing personal data must be secured in a manner consistent with this policy.

Disposition/Destruction of Information

Paper and electronic records containing personal data must be disposed by a secure and approved method that is understood by all staff or authorised persons.

Any temporary or permanent staff who leave the school must return all records containing personal data, in any form, which may at the time of such termination be in the former person's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

Training

A copy of this Policy will be distributed to each employee or authorised person, (as well as visitors and suppliers as appropriate), who will have access to personal data. All such persons shall, upon receipt of the Policy, acknowledge in writing that he/she has received, read and understood it.

When the Policy is first issued, there will be training for employees and temporary employees who have access to personal data on the detailed provisions of the policy. All employees shall be retrained regularly.

All attendees at such training sessions are required to certify their attendance at the training and their familiarity with the company's policy and procedures for the protection of personal data.

Breaches

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 to the School Business Manager and the 'Breach and Non-Compliance' procedure is to be followed.

Third Parties

The contents of this Policy will apply to third parties who are intended to receive and process personal data.

Exceptions

Any exceptions to this policy require prior written authorisation and approval from the Headteacher.

Approved by Governors at full governing body meeting 25.11.21

Reviewed at Resources Committee Meeting 30.6.22

This Policy is due for review in June 2023.

Schedule 1

Good Practice Guide

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.

To do this we are all responsible for personal data when it is in our control.

Keeping Records Secure

All records that include pupil/staff identifiable information will be stored appropriately, which may include securely in locked filing cabinets, password protected electronic databases or another form of restricted access storage when not in use depending on the sensitivity of the information contained in the records.

Employees are expected to take appropriate measures to ensure the security of personal data at all times, including keeping records secure when attending meetings or removing records from site to work on at home.

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 school-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. (see appendix 2)

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 considered at all times when recording, sharing, deleting or withholding information.

Sensitive information must not be shared unless the person is authorised to receive it.

Email and Electronic sharing

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 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 considered to be highly sensitive.

EMPLOYEE ACKNOWLEDGEMENT FORM

I have received, read and understand the Information Security Policy. I understand that it is my responsibility to comply with it.

Printed name: _____

Signature:_____

Date:_____

A SECURITY BREACH is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the school.

Please return this form to the School Business Manager