[SCHOOL] INFORMATION SECURITY POLICY

1 POLICY OBJECTIVES

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) aim to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

[SCHOOL] is dedicated to ensure the security of all information that it holds. The School will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. The School will develop, implement and maintain safeguards appropriate to its available resources, the amount of personal data that it holds and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

All staff are responsible for keeping information secure in accordance with the relevant legislation and must follow the School's Acceptable Usage Policy (AUP).

This policy sets out the measures taken by *[SCHOOL]* to achieve this, including to

- protect against potential breaches of confidentiality;
- ensure that all information assets and ICT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility for staff to protect the confidentiality and integrity of the information that they themselves handle.

1.1 Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the School's Data Protection Policy, Data Breach Policy, Acceptable Usage Policy, Remote Working Policy, Remote Learning Policy and *[INSERT AS APPROPRIATE]* for further information. These policies are also designed to protect personal data and can be found on the School website, on the staff shared network and *[INSERT AS APPROPRIATE].*

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, smartphones, laptops, tablets, digital cameras and memory sticks.

1.2 Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of *[SCHOOL]*, in whatever media. This includes information held in computer systems, emails, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence that may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

1.3 General principles

All data stored in the School's ICT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data, special category personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Data Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with their line manager *[and/or the Data Protection Lead]* the appropriate security arrangements for the type of information they access in the course of their work.

2 ROLES AND RESPONSIBILITIES

2.1 *[GOVERNORS/TRUSTEES]*

[GOVERNORS/TRUSTEES] retain the ultimate responsibility and accountability for compliance with the relevant legislation. They must ensure that sufficient resources are available to maintain the security of the information held by the School. This should include having a business continuity plan in place that has cyber resilience as a consideration.

[GOVERNORS/TRUSTEES] should ensure that they are aware of the latest high level advice and guidance available from organisations such as the National Cyber Security Centre.

2.2 HEADTEACHER

The Headteacher is responsible for ensuring day-to-day compliance with the relevant legislation and the implementation of this Policy. The Headteacher will ensure that all staff are familiar with all aspects of this Policy including the consequences of failing to comply with the requirements.

2.3 MEMBERS OF STAFF

All members of staff must comply with all relevant parts of this policy at all times when using ICT Systems.

Computers and other electronic devices should be locked when not in use to minimise the risk of accidental loss or disclosure of data.

Staff must immediately inform *[INSERT JOB TITLE AS APPROPRIATE]* of any and all security concerns relating to the ICT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the ICT Systems must be reported to the *[INSERT JOB TITLE AS APPROPRIATE]* immediately.

Staff must not install any personal software without the approval of the *[INSERT JOB TITLE AS APPROPRIATE]*. Any personal software may only be installed where that installation poses no security risk to the ICT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Staff must ensure that any physical media (e.g. USB memory sticks or disks of any kind) used to transfer files is virus-scanned before use. *[INSERT JOB TITLE AS APPROPRIATE]*'s approval must be obtained prior to transferring of files using cloud storage systems.

If a member of staff detects any virus this must be reported immediately to *[INSERT JOB TITLE AS APPROPRIATE]* even where anti-virus software automatically resolves the issue.

All staff have an obligation to report actual and potential data protection compliance failures to the Data Protection Lead (DPL) for further investigation of the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data must be reported to the Data Protection Officer (contact details for the DPO can be found in the School's Data Protection Policy).

Members of staff must not attempt to resolve an ICT security breach on their own without first consulting *[INSERT JOB TITLE AS APPROPRIATE].*

2.4 SPECIALIST TECHNICAL STAFF

[INSERT AS APPROPRIATE including details covering the following responsibilities:

- *ensuring that all ICT Systems are assessed and deemed suitable for compliance with the School's security requirements;*
- *ensuring that ICT Security standards within the School are effectively implemented and regularly reviewed;*
- *assisting members of staff in understanding and complying with this Policy;*
- *providing all members of staff with appropriate support and training in ICT Security matters and use of ICT Systems;*
- *ensuring that all members of staff are granted levels of access that are appropriate to their job role, responsibilities, and any special security requirements;*
- *receiving and handling all reports relating to ICT Security matters and taking appropriate action in response, including, in the event that any reports relate to personal data, informing the Data Protection Officer;*
- *taking proactive action, where possible, to establish and implement ICT Security procedures and raise awareness among members of staff;*
- *monitoring all ICT security within the School;*
- *ensuring that regular backups are taken of all data stored within ICT Systems at regular intervals and that such backups are stored at a suitable location offsite.]*

3 TECHNICAL MEASURES

The School has put in place the technical measures detailed in Annex 1 of this policy *[INSERT ANNEX 1 AS APPROPRIATE following consultation with relevant technical staff]*

4 ORGANISATIONAL MEASURES

4.1 Physical security and procedures

All data stored in the School's ICT Systems and paper records will be available only to members of staff with legitimate need for access and will be protected against unauthorised access and/or processing and against loss and/or corruption.

Paper records and documents containing personal information, sensitive personal information, and confidential information must be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when a desk or office is unoccupied, all paper documents must be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks must be used to store paper records when not in use.

Paper documents containing confidential personal information must not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. Particular care must be taken if documents have to be taken out of school.

The physical security of buildings and storage systems will be reviewed on a regular basis. Any member of staff who finds security to be insufficient, must inform *[INSERT JOB TITLE AS APPROPRIATE]* as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The School will carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School has made the following arrangements to minimise the risk of unauthorised people from entering the school premises:
[INSERT AS APPROPRIATE including details of opening hours, alarm systems, CCTV, signing–in protocols etc]

4.2 Access security
All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this Policy.

The School has technical measures in place that prevent individuals from unauthorised access and protect the School's network. The School also teaches individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All ICT Systems (in particular mobile devices) must be protected with a secure password or passcode, or such other form of secure log-in system as approved by *[INSERT AS APPROPRIATE].*

Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) must be protected with a screen lock that will activate after a period of inactivity. Staff must not change this time period or disable the lock. All mobile devices provided by the School, will be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of login to unlock, wake or similar.

Staff who fail to log off and leave their terminals unattended could be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

4.3 Password protocol
[INSERT AS APPROPRIATE. The following is an example only:
All passwords must, where the software, computer, or device allows:

- *be at least 6 characters long including both numbers and letters;*
- *be changed on a regular basis and at least every 180 days;*
- *not be the same as the previous 10 passwords you have used;*
- *not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)*

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the [INSERT JOB TITLE AS APPROPRIATE] as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify the [INSERT JOB TITLE AS APPROPRIATE] to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. Passwords should never be left on display for others to see.]

4.4 Data security
Personal data sent over the School network must be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from *[INSERT JOB TITLE AS APPROPRIATE]*. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's ICT systems.

Staff may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi in line with the Schools Acceptable Usage Policy. The School reserves the right to request the immediate disconnection of any such devices without notice.

4.5 Electronic storage of data
All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by *[INSERT JOB TITLE AS APPROPRIATE]*.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

Personal data should not be stored on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the [INSERT JOB TITLE AS APPROPRIATE]. Data copied onto any of these devices should be deleted as soon as possible once it is stored on the School's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day by *[INSERT JOB TITLE AS APPROPRIATE].*

4.6 Communication and transfer of data
All personal data, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by [INSERT DETAILS OF SECURE METHOD] or recorded delivery.

Postal, secure exchange and email addresses and numbers should be checked and verified before any information is sent to them. Extra care must be taken with email addresses where auto-complete features may have inserted incorrect addresses.

Confidential information should be clearly marked as such and only circulated to recipients who need to know the information in the course of their work for the School. Confidentiality should also be maintained when speaking in public places.

Personal or confidential information should not be removed from the School without prior permission from *[INSERT JOB TITLE AS APPROPRIATE]* and only where the removal is temporary and necessary. When such permission is given all reasonable steps must be taken to ensure that the integrity of the information and the confidentiality are maintained. Personal or confidential information must not be:

- transported in see-through or other un-secured bags or cases;
- read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

4.7 Reporting security breaches

All concerns, questions, suspected breaches, or known breaches must be referred immediately to *[INSERT JOB TITLE AS APPROPRIATE]* and the Data Protection Officer (DPO) if the incident involves personal data. All members of staff have an obligation to report actual or potential data protection compliance failures. Full details on how to report data breaches are set out in the Breach Notification Policy.

When receiving a question or notification of a breach, *[INSERT JOB TITLE AS APPROPRIATE]* will immediately assess the issue, including but not limited to, the level of risk associated with the issue, and will take all steps necessary to respond to the issue.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to *[INSERT JOB TITLE AS APPROPRIATE].*

All ICT security breaches must be fully documented.

5 REMOTE WORKING AND TEACHING

5.1 Working from home

Staff should not take confidential or other information home without prior permission of *[INSERT JOB TITLE AS APPROPRIATE]*, and only do so when satisfied that appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

Staff who have been given permission to take confidential or other personal information home, must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

Following the increase in working from home resulting form the Covid-19 health emergency, all staff should have due regard for

- Annex 2: Protocol for Protecting Personal Data When Working Remotely
- Annex 3: Home Working: Managing the Cyber Risks (NCSC)
- Annex 4: Remote Working: A guide for education professionals (SWGfL)

5.2 Remote Teaching

Staff must follow the School's Policy for Remote Learning when delivering live or recorded lessons online.

Where staff are delivering online lessons from home they must comply with all the conditions outlined in 5.1 Working from Home.

6 Related Policies

Staff should refer to the following policies that are related to this Information Security Policy:

- Safeguarding Policy
- Acceptable Usage Policy;
- Data Breach Notification policy;
- Data Protection Policy
- Remote Learning Policy
- *[INSERT AS APPROPRIATE]*

ANNEX 1:
TECHNICAL MEASURES

ANNEX 2:
Protocol for Protecting Personal Data When Working Remotely

Devices

- Take extra care that devices, such as USBs, phones, laptops, or tablets, are not lost or misplaced,
- Make sure that any device has the necessary updates, such as operating system updates (like iOS or android) and software/antivirus updates.
- Ensure your computer, laptop, or device, is used in a safe location, for example where you can keep sight of it and minimise who else can view the screen, particularly if working with sensitive personal data.
- Lock your device if you do have to leave it unattended for any reason.
- Make sure your devices are turned off, locked, or stored carefully when not in use.
- Use effective access controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict access to the device, and to reduce the risk if a device is stolen or misplaced.
- When a device is lost or stolen, you should take steps immediately to ensure a remote memory wipe, where possible.

Emails

- Follow the School's policies around the use of email.
- Use work email accounts rather than personal ones for work-related emails involving personal data. If you have to send personal data make sure contents and attachments are encrypted and avoid using personal or confidential data in subject lines.
- Before sending an email, ensure you're sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data.

Cloud and Network Access

- Only use the School's trusted networks and cloud services, and comply with all rules and procedures about cloud and network access, login and, data sharing.
- If you are working without cloud or network access, ensure any locally stored data is adequately backed up in a secure manner.

Paper Records

- It's important to remember that data protection applies to not only electronically stored or processed data, but also personal data in manual form (such as paper records) where it is, or is intended to be, part of filing system.
- Where you are working remotely with paper records, take steps to ensure the security and confidentiality of these records, such as by keeping them locked in a filing cabinet or drawer when not in use, disposing of them securely (e.g. shredding) when no longer needed, and making sure they are not left somewhere where they could be misplaced or stolen.
- If you're dealing with records that contain special categories of personal data (e.g. health data or social care data) you should take extra care to ensure their security and confidentiality, and only remove such records from a secure location where it is strictly necessary to carry out your work.
- Where possible, you should keep a written record of which records and files have been taken home, in order to maintain good data access and governance practices.

ANNEX 3:
Home Working: Managing the Cyber Risks (NCSC)

ANNEX 4:
Remote Working: A guide for education professionals (SWGfL)