Information Security Policy

St Peter's School, York

April 2026

(Next review Christmas Term 2027)

Introduction

The UK General Data Protection Regulation (UK GDPR) aims 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.

The School endeavours to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the School to achieve this, including to:

- protect against potential breaches of confidentiality.
- ensure that all information assets and IT 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 of staff to protect the confidentiality and integrity of the information that they handle.

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

Information security includes cyber security, which encompasses the protection of the School's digital systems, online services, user accounts, and data from cyber threats such as unauthorised access, phishing, malware and system compromise. The School recognises the importance of cyber security in maintaining the integrity of examination processes and meeting the requirements of awarding bodies and the Joint Council for Qualifications (JCQ).

Staff are referred to the School's Data Protection Policy, Data Breach Policy and, Staff IT Acceptable Use Policy for further information. These policies are also designed to protect personal data and can be found on the Staff Homepage.

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, laptops, tablets, digital cameras, memory sticks and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, emails, paper records, hand-held devices, and information transmitted orally. The examples are not exhaustive and there may other records and information which may be considered personal data.

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 which 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 to remain compliant with legal obligations. This includes staff who access awarding organisations' online systems or any systems containing examination-related information. This policy applies to staff involved in the management, administration and conducting of examinations and assessments, and to all staff who access awarding bodies' online systems for the purposes of delivering or supporting the examinations process.

General Principles

All data stored on our IT Systems are to be classified appropriately (including, but not limited to, personal data, sensitive 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 Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Cyber security controls must be proportionate to risk and aligned with recognised guidance, including National Cyber Security Centre (NCSC) advice and JCQ requirements relating to examination systems.

Staff should discuss with the IT Operations Manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by IT Department or by such third party/parties as the IT Department may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the IT Operations Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Senior Deputy who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Cyber security controls and practices, including those relating to examination systems, will be reviewed at least annually, or following a significant cyber incident, to ensure continued compliance with current best practice and JCQ requirements.

In relation to examination systems, the School will act in accordance with JCQ General Regulations for Approved Centres and associated guidance on cyber security.

Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the

working day, or when staff leave their desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use. If staff do not feel they have the appropriate and/or sufficient storage available, they must inform the Estates Manager as soon as possible.

If the papers contain personal data then they must be kept in secure cabinets when not being used.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or on noticeboards outside of a classroom. Noticeboards located inside classrooms can contain pictures and first names of students, but no other personal data.

Particular care must be used if documents must be taken out of school.

Please do not print documents containing Personal Data unless it is required for a specific purpose and ensure that any documents are shredded once the need for the information is passed.

To reduce the risk of documents containing sensitive information being printed out but not collected, the school encourages the use of “follow-me printing”. If this is not available to staff, please ensure that staff collect documents immediately when printing them out. If staff see anything left by the printer which contains School Personal Data then staff must hand it in to the Data Manager.

When no longer needed, paper records containing personal data should be shredded and disposed of securely by placing them in confidential waste bags. Documents containing personal data should never be placed in the general waste. Confidential waste bags should not be left unattended or kept in an area which can be accessed by students or the public.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If staff find the security to be insufficient, staff must inform the Director of Operations as

soon as possible. Increased risks of vandalism and or burglary shall be considered when assessing the level of security required.

The following measures are taken by the School to ensure physical security of the buildings and storage systems:

- The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.
- The School has an intercom system on the main receptions to each school to minimise the risk of unauthorised people from entering the school premises.
- Access to school buildings is restricted to authorised persons by an electronic access control system. Alarm systems are fitted to key buildings and set out of school working hours.
- CCTV Cameras are in use at the School and monitored.
- Visitors are required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Computers and IT

The IT Operations Manager shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;
c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990.
d) Monitoring account activity, managing connected applications, reviewing system security settings regularly, and ensuring secure configuration of systems used to access external services, including awarding bodies' platforms.

Furthermore, the IT Operations Manager, with the support of the Data Manager, shall be responsible for the following:

a) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
b) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
c) receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Data Protection Officer;
d) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
e) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
f) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are suitably stored offsite.

Multi-Factor Authentication (MFA) is mandatory for all systems that contain examination-related information or provide access to awarding bodies' online services. Staff must ensure MFA is correctly set up and always used and report issues immediately to the IT Operations Manager.

The School will maintain an up-to-date device and account asset register covering all computers, mobile devices and user accounts used in the administration and conducting of examinations. Devices on this register must have up-to-date anti-malware protection and security updates applied, in line with JCQ requirements.

Systems used to access cloud-based services, including email, storage and awarding-body platforms, must be securely configured, regularly reviewed and monitored, with access restricted to authorised personnel only.

Responsibilities – Members of Staff

Cyber security training must cover, as a minimum:

- creating strong, unique passwords;
- keeping account credentials strictly confidential;
- the importance and correct use of Multi-Factor Authentication (MFA);
- recognising phishing and other forms of social engineering; and
- the importance of promptly reporting suspicious activity or incidents.

The School will download and retain certificates of cyber security training completion for all relevant staff, and these certificates will be made available for inspection on request by JCQ or any awarding body.

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

Staff must immediately inform the IT Operations Manager and Data Manager of all security concerns relating to the IT Systems which could or has led to a data breach.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the IT Operations Manager immediately.

No software should be installed unless purchased by the school to avoid licencing breaches.

Prior to installation of any software onto the IT Systems, check with the IT Systems and Data Manager as appropriate to confirm if a Data Privacy Impact Assessment is needed and for approval of the software.

Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, staff must make sure to have the physical media virus scanned. Approval from IT Operations Manager must be obtained prior to transferring of files using cloud storage systems.

If staff detect any virus this must be reported immediately to the ICT Support Desk (this rule shall apply even where the anti-virus software automatically fixes the problem).

If staff use a "virtual classroom" which allows staff to upload lesson plans and mock exam papers for pupils then staff need to be careful that staff do not accidently upload anything more confidential;

Staff must know how to use properly any security features contained in School software. For example, some software will allow staff to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that staff can use this software correctly so that the recipient of the document cannot "undo" the redactions; and staff need to be very careful where staff store information containing Special Category Personal Data, if in doubt, speak to the Data Manager.

- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it must be encrypted.
- Use of personal email accounts or unencrypted personal devices by governors, staff or contractors for official School business is not permitted.

Roles and Responsibilities - Exams Delivery

All members of staff must always comply with all relevant parts of this policy when using the IT Systems and complete annual cyber security training. This training must remain up-to-date, and staff must not access secure systems where training has lapsed.

Governors

- Oversee and review cyber security arrangements relating to the administration and delivery of examinations.
- Ensure appropriate assurance is sought regarding cyber security risks linked to awarding-body systems.

Senior Leadership Team

- Hold overall accountability for cyber security relating to examinations.
- Ensure an up-to-date asset register is maintained for all devices and user accounts used for the administration and conducting of examinations.
- Ensure all staff who access awarding-body systems complete annual, certificated cyber security training and that certificates are retained for inspection.

Exams Officer and Exams Staff

- Follow all cyber security requirements relating to awarding-body systems.
- Comply with account-management best practice for exam-related systems.
- Report any suspicious activity, attempted compromise or security incident immediately to the IT Operations Manager and the relevant awarding body if appropriate.

Invigilators

- Comply with all centre instructions relating to secure handling, access and reporting of any concerns regarding exam-related digital materials or systems.

IT Operations Manager / IT Team

- Implement technical controls for all exam-related systems, including secure configuration of cloud platforms and awarding-body interfaces.

- Monitor and audit account activity on exam systems, regularly review access permissions and remove access promptly when no longer required.
- Maintain the exams device and account asset register and ensure devices remain patched, updated and protected by anti-malware solutions.
- Lead the technical response to any cyber security incident impacting examinations.

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 a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to 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 IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

All passwords must, where the software, computer, or device allows:

a) be at least 10 characters long including 3 of the following upper case, lower case, numbers, or special character;
b) when changed, cannot be the same as the previous passwords staff have used;
c) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Any password believed to have been exposed or compromised must be changed immediately and reported to the IT Operations Manager. Where supported, secure account recovery options must be enabled for systems containing examination related data.

Account Management – Exams Systems

Staff who access awarding-body or exam-related systems must:

1. Use strong, unique passwords for each system used.

2. Keep all account details, passwords and MFA codes strictly confidential.
3. Enable Multi-Factor Authentication and any additional security settings provided.
4. Change any password that may have been exposed and report the exposure immediately.
5. Set secure account recovery options where supported by the system.
6. Review and remove unnecessary connected applications or integrations.
7. Monitor their own account activity and immediately report any suspicious or unauthorised access.

Passwords must be kept confidential and must not be made available to anyone else. Any member of staff who discloses their 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 uses another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If staff forget their password staff should contact the IT Support Team to have their access to the IT Systems restored. Staff must set up a new password immediately upon the restoration of access to the IT Systems.

Staff should not write down passwords if it is possible to remember them. If necessary, staff may write down passwords provided that staff store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. Staff may not change this time period or disable the lock.

All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. Staff may not alter this period.

Staff should be aware that if they fail to log off and leave their terminals unattended or unlocked, they may 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.

User access rights are reviewed regularly and linked to the school's MIS (iSAMS). Access will be removed promptly when a member of staff changes role or leaves the School. For awarding-body and examinations systems, account activity is monitored and auditable. Permissions are reviewed at appropriate intervals to ensure minimum-necessary access, and access is removed promptly when no longer required.

Data Security

Connected applications and data integrations must be reviewed and approved to ensure they do not introduce cyber security risks.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from IT Operations Manager.

Staff may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that staff follow the IT Departments requirements and instructions governing this use. All usage of staff's own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The IT Manager may at any time request the immediate disconnection of any such devices without notice.

If staff are granted access to a database containing records of multiple individuals, staff must only access the records of individuals for whom staff have a legitimate business reason to do so. It is an offence under the Computer Misuse Act (1990) to access the data of other individuals without authorisation.

Electronic Storage of Data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by IT Operations Manager.

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

All data is securely backed up daily and is the responsibility of the IT Operations Manager.

Home-Working and off site

Staff should ensure that appropriate technical and practical measures are in place within their home to maintain continued security and confidentiality and must ensure that:

a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

b) 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.

When using school systems from personal devices staff much not generating reports and exports etc. that will automatically download to their machine. If this processing is essential, ensure that these downloads are deleted after use.

The School recognises that there may be a very few occasions when it is expedient to use their own mobile device for school purposes. For example, to contact a parent about their child in an emergency whilst on a School trip. However, as soon as staff return to School Staff should transfer or delete any School Personal Data.

Communications, Transfers, Internet and Email Use

When using the School's IT Systems staff are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to IT Operations Manager.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the School cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery. Staff may not send information by fax. Attachments containing Special Category data should also be password protected and the password sent in a separate email for both internal and external emails. When sending emails containing sensitive information ask a colleague to check the email.

Postal, DX, and email addresses and numbers should be checked and verified before staff send information to them. Staff should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

Staff should be careful about maintaining confidentiality when speaking in public places.

Staff should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the school without prior permission from a member of the St Peter's Leadership Team except where the removal is temporary and necessary. When such permission is given staff must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. Staff must ensure that the information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Staff must not use a private email address for School related work. Staff must only use their @stpetersyork.org.uk address.

Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Data Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.

Any actual or suspected compromise of an awarding body's online systems, or credentials used to access such systems, must be reported immediately to the relevant awarding body and to the IT Operations Manager.

When receiving a question or notification of a breach, the Data Manager and Senior Deputy shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the IT Operations Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the IT Operations Manager.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to IT Operations Manager, Data Manager and Senior Deputy.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.

Cyber Incident Response

In the event of a cyber security incident, including phishing attacks, unauthorised access or suspected system compromise, the IT Operations Manager will lead the technical response, working with the Data Manager, and Data Protection Officer as appropriate.

If a cyber incident affects learner data, assessment records or candidate work, the School will contact the relevant awarding body immediately for advice and support, in addition to following the incident response process set out above.

Related Policies

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

- Data Breach Policy;
- Data Protection Policy

Authorised by	The Head Master
Reviewed by	SPLT April 2026
Next Review	Christmas Term 2027