Information Security Policy

St Peter's York

December 2024

(Next review Christmas term 2026)

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 is dedicated 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.

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 and Electronic Information and Communication Systems Policy, ICT 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 in order to remain compliant with legal obligations.

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.

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).

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 you leave your 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 you do not feel you have the appropriate and/or sufficient storage available to you, you must inform the Estate Manager as soon as possible.

If the papers contain **Critical School 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 pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents must be taken out of school.

Please do not print documents containing School 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.

When printing documents, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains School Personal Data then you must hand it in to the Data Manager. The School uses “follow me” printing which means that you cannot print something out unless standing by the printer.

Paper records containing School Personal Data should be shredded and disposed of securely by placing them in datashred bags. School Personal Data should never be

placedin the general waste. Datashred bags should not be left unattended.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Director of Operations as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the School to ensure physical security of the building/s 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 to minimise the risk of unauthorised people from entering the school premises.
- The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.
- CCTV Cameras are in use at the School and monitored by Head of Facilities.
- Visitors should be 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.

Furthermore, the Data Manager shall be responsible for the following:

a) with the support of the IT Team, assisting all members of staff in understanding and complying with this policy;
b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;

c) 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;
d) 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;
e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
f) 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
g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of Staff

All members of staff must always comply with all relevant parts of this policy when using the IT Systems.

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

You must immediately inform It Operations Manager and Data Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

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 Data Manager to confirm if a Data Privacy Impact Assessment is needed. You must obtain written permission from a member of the St Peter's Leadership Team and IT Operations Manager for approval of the software. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you 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 you 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 you use a "virtual classroom" which allows you to upload lesson plans and mock exam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;

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

- no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
- 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 will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices by governors, staff or contractors for official School business is not permitted.

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 teach 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) be changed on a regular basis ;
c) cannot be the same as the previous 10 passwords you have used;
d) 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 IT Manager as appropriate and necessary. 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 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 contact the IT Support Team 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. If necessary, you may write down passwords provided that you 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 electronical 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. You 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. You may not alter this time period.

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

Data Security

Personal data sent over the School network will 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 IT Operations Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given, all files and data should always be virus checked before they are downloaded onto the School's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the IT Departments requirements and instructions governing this use. All usage of your 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 you are granted access to a database containing records of multiple individuals, you must only access the records of individuals for whom you 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.

You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Senior Deputy Head You should delete data copied onto any of these devices as soon as possible and make sure 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 and is done by IT Operations Manager

Except for EYFS there maybe occasions where games coaches can record movements so that they can be analysed using apps such as Coach Eye. Explicit consent must be sought from parents and students (depending on age) for recordings to be taken on personal devices and must be transferred to the school network or deleted within 3 days of the recording date.

Home-Working and off site

You should not take confidential or other information home without prior permission of a member of the St Peter's Leadership Team, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you 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 electronical material, securely destroyed, as soon as any need for its retention has passed.

When using iSAMS from home try to avoid generating reports and exports etc. When doing so these reports will automatically download to your 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 your 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 you return to School you should transfer or delete any School Personal Data.

Communications, Transfers, Internet and Email Use

When using the School's IT Systems you 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. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine. 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, fax and email addresses and numbers should be checked and verified before you send information to them. You should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

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

You 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 you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

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

You must not use a private email address for School related work. You must only use your @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.

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.

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 December 2024
Next Review	Christmas Term 2026