St Peter's College

Information Security Policy - Summary

Contents

Revision History

Version	Date	Author	Description of Changes
0.4	**1/11/15**	**JG**	**Various drafting changes throughout (Bursar, FD, IT Manager)**
0.5	**26/11/15**	**JG**	**Various drafting edits throughout (Bursar, IT Fellow)**
0.6	**6/11/18**	**JG**	**Various drafting edits throughout, reflecting GDPR, IT Maturity Assessment, use of personal email addresses, academic freedom (GB minute reference 15259).**
0.7	**19/11/18**	**JG**	**To note that v0.6 was approved by DPO (ClearComm) 8/11/18. Minor edits made.** **Approved by Governing Body 28 November 2018**

St Peter's College

Information Security Policy – Summary

Aims and responsibilities

- The aims of information security are to protect the availability, utility and confidentiality of information and to ensure compliance with legal requirements.
- The Bursar is responsible for ensuring that St. Peter's College complies with this policy and all other University policies and procedures relating to information security.
- St. Peter's College shall protect the security of its information and information systems and use a risk-based approach to decide the appropriate level of control.
- St. Peter's College shall ensure that all users receive appropriate training and education in information security.

Procedures and practices

- Mobile devices used to handle confidential information - laptops, tablets, smartphones, memory sticks, etc. - must be appropriately secured. If they cannot be secured, they must not be used to handle confidential information.
- E-mail is not a secure form of communication. Users wishing to send confidential information should consider using more secure methods, or at least minimise the amount sent this way. Where no suitable alternative to e-mail exists, appropriate safeguards should be taken e.g. encryption or password protection.
  See IT Services Securing Email http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/email-and-exchange-information#d.en.111095
- Personal email accounts must not be used for college or university business.
- Confidential information should not be stored in e-mail folders, as it is not secure. If an email or email attachment contains information that needs to be kept, you should save it to a secure area of the network.
- Confidential information should be stored in the file share, Zinc, and not on local hard drives. If local hard drives are used they must be encrypted.
- Confidential information should be downloaded from secure University systems (e.g. OSS, Oracle Financials, DARS) only when strictly necessary, and deleted after use.
- Passwords must not be shared (except where specifically authorised by line management) or easy to guess.
- Home computers used to access University systems must be kept secure through firewalls, anti-virus software and security updates. The College reserves the right to inspect computers used for College purposes in the event of clear evidence of misconduct, an official complaint or in relation to a breach or incident that has been reported to the ICO (Information Commissioner) by the DPO (Data Protection Officer).
- Critical files must be backed up.
- Envelopes containing confidential documents must be sealed securely and addressed correctly and, in the case of external mail, sent by recorded delivery.
- Confidential information must be removed from redundant or surplus IT equipment or office furniture before disposal; redundant hard drives are securely destroyed.
- Appropriate physical measures must be taken to prevent the theft, loss or inadvertent exposure of confidential data e.g. lock computer screens when not at your desk, lock away hard copy confidential documents, do not read confidential information in a public place where it can be viewed by others.
- Any security incidents must be reported promptly.

Part 1 – Aims and Responsibilities

1 Policy Statement

St. Peter's College is committed to protecting the security of its information and information systems.

The information it manages shall be appropriately secured to prevent breaches of confidentiality, failures of integrity or interruptions to the availability of that information, as well as to ensure appropriate compliance.

St. Peter's College shall provide education and training in information security and raise awareness of its importance.

To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

All colleges have developed Information Asset Registers and completed an Information Maturity Assessment Exercise to benchmark data and systems security. This was carried out first in 2017 and recently in August 2018. GDPR has also been implemented in May 2018. Our GDPR DPO has carried out our first GDPR Gap Analysis and Audit in August 2018. This document has been updated where necessary to reference these developments.

Specialist advice can be sought via the University's Information Security Team (https://www.infosec.ox.ac.uk/welcome) and/or OxCERT (https://help.it.ox.ac.uk/service/oxcert.)

2 Importance of information security

St. Peter's College's computer and information systems underpin St. Peter's College's activities. St. Peter's College recognises the need for its staff, students, visitors and contractors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this. Security of information is essential to maintaining the continuity of its business activities and to its compliance with University regulations and policies.

3 Purpose

This policy supplements the University's overarching policy and defines the framework within which information security will be managed across St Peter's College. It is the primary College policy under which all other technical and security related polices reside. **Annex A** provides a list of all other policies and procedures that support this policy.

4 Scope

This policy is applicable to and will be communicated to all staff, members and other relevant parties who use College IT systems and services (e.g. visitors, conference guests, contractors, summer school staff and students etc). It covers, but is not limited to, any systems or data attached to the St. Peter's College's computer or telephone networks, any systems supplied by the St. Peter's College, any communications sent to or from St. Peter's College and any data - which is owned either by the University or St. Peter's College- held on systems external to the St. Peter's College's network.

5 Roles and responsibilities

The Bursar is ultimately responsible for the maintenance of this policy and for its implementation within the St Peter's College.

The IT and Web Committee is responsible for reviewing this policy annually for FACo and GB review and approval. The committee will provide direction and support and promote information security through appropriate commitment and adequate resourcing.

The IT Manager is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy.

Administrative department line managers are responsible for the security and integrity of the data they process and control.

It is the responsibility of all administrative department line managers within St Peter's College to ensure that all staff for which they are responsible are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each employee to comply with this policy, and with all other policies and procedures relating to information security. If someone is uncertain whether a particular activity is permissible under this or related policies, they should consult the IT Manager.

IT security incidents should be reported to the IT Manager who will escalate as necessary. Data incidents and breaches should be reported to the DPO who will escalate as necessary, and in cetain cases report them to the Information Commissioner's Office (ICO).

Part 2 – Detailed Procedures and Practices

Part 2 is directed at users and sets out the procedures and practices you need to follow in order to implement the objectives identified in Part 1, particularly in relation to the protection of confidential information. The appropriateness of some procedures or practices will depend on the results of the College's risk assessment.

6 Definition of confidential information

For this purpose, confidential information is any information that is not intended to be publicly available. If the loss or unauthorised disclosure of information could have adverse consequences for the University, the College or individuals, it is confidential.

Given the potentially serious consequences of breaching the GDPR, you should assume that all personal data is confidential. (Personal data is any data that identifies a living individual eg a CV, email address, reference, job or course application, home contact details, etc.)

Examples of confidential information, involving both personal data and business information, are at **Annex B.**

7 Use of mobile devices

General

The use of mobile devices (laptops, St Peter's College encrypted USB sticks, smart phones, tablets, etc.) is an area of high risk, because they can be easily lost or stolen. It is essential that such devices be appropriately secured.

You should apply the latest security patches to your device.

When using your device on an unsecured public Wi-Fi network you must use the University VPN service (or similar local departmental service) in order to ensure a secure connection to the University network. Further information is available at http://help.it.ox.ac.uk/network/vpn/index

Applications should be installed only from trusted locations.

Any equipment that is taken off College property, especially laptops, must be kept secure and should not be left unattended at any time. In the event of any loss or theft, you are to inform the IT Department immediately.

All employees are required to take reasonable measures to minimise the risk of loss of College data and software through theft.

Should you receive in portable format (e.g. CD or USB drive), you must ensure that it is virus checked before being loaded onto the College's system. You should contact the IT Department who will conduct a virus check and give you confirmation that it is safe to use.

Encryption of laptops and St Peter's College encrypted USB memory sticks

All devices that might be used to hold sensitive or confidential data must be encrypted. The University has implemented a PGP Whole Disc Encryption (WDE) service (http://www.it.ox.ac.uk/infosec/wde/). Portable/removable storage media such as USB drives holding sensitive or confidential data must employ hardware encryption. These work like normal USB devices, but require a password to access data and are available through the College IT department. The University WDE service is not currently appropriate for tablets and smartphones; advice on how to make these more secure is available from the IT Manager. Some devices may have built-in encryption capabilities.

Other devices (Tablets, Smartphones)

There are a range of ways to secure other devices and if the device is to be used to handle confidential information, it must be appropriately secured, in accordance with the principles stated in InfoSec's 'Stay Safe on the Move' site (https://www.infosec.ox.ac.uk/stay-safe-move.). If this cannot be done, you must not use the device to hold or transmit confidential data.

8 Information Exchange (including Email and Cloud Services)

The College has subscribed to the statements regarding computing and network rules, etiquette and security by the University of Oxford IT Services Department on behalf of the University of Oxford. Employees and members should ensure that they follow these statements at all times. Please see https://www.it.ox.ac.uk/rules for further details.

The College has subscribed to the policies of JANET (Joint Academic Network). Employees should ensure that they follow these statements at all times. Please see https://community.ja.net/library/library for further details.

The College recognises that commercial data is a valuable asset and as such, you should not distribute this sensitive data to third parties. Doing so will constitute gross misconduct potentially resulting in summary dismissal.

Confidential information about or relating to the business of the College, its members, suppliers and or contacts, should not be transmitted outside the College via email or otherwise, unless done so in the course of business and without due authorisation. Confidential information should not be left on display on an unattended workstation.

E-mail

E-mail is not a secure form of communication, and ideally, you should not use it to send confidential information or at least minimise the amount you send in this way.

Once you join the College, if appropriate you will be provided with a University email account. This account can send and receive emails from anyone connected to the internet.

Personal email accounts must not be used for college or university business.

You should first consider communicating confidential information by a more secure method than e-mail. If a suitable alternative is not available, you should consider encrypting the message and/or attachment.

See InfoSec's 'Stay Safe on Email' https://www.infosec.ox.ac.uk/stay-safe-on-email

You must ensure that emails containing confidential data are sent to the correct address and not rely solely on any 'autocomplete' function. You should take particular care when selecting an address from a directory.

If you receive confidential information inadvertently via e-mail, you should delete it as soon as possible.

Confidential information should not be stored in e-mail folders, as it is not secure. If an e-mail or e-mail attachment contains information that needs to be kept, you should save it to a secure area of the network.

Sending or receiving of defamatory or pornographic content that in any way contravenes either UK or European law is forbidden and could result in disciplinary action.

Any emails received with offensive, demeaning, disruptive or illegal attachments are expected to be deleted along with any attached content and not forwarded onto others. The sender of the message should be informed or the College's email policy.

You should ensure that at least once a month a clear up of your email account is done and any unwanted emails are deleted.

You should be aware that these deleted emails will remain on the system for a period or 14 days, and will be accessible from backup should you mistakenly delete an email or, if an investigation into network abuse needs to be commenced.

The College reserves the right to access and monitor any or all areas of its computer network for business reasons and training purposes. You should not assume that any information held on the College or University system is private.

If you suspect that any of your email accounts have been compromised, you are to report this immediately to the St Peter's College IT Department and, if applicable, your manager.

Employees should take all reasonable steps to ensure that emails they send to do not contain a virus, malware, zombies and Trojans.

Emails sent must not adversely affect the College's business operation, safety of its members, and its public image.

Emails sent externally must contain the College email disclaimer, which can be obtained from the IT department.

If you receive an email, with or without an attachment from an unknown source, or “junk” email, you should delete it immediately upon receipt without opening it. Opening such as email may leave the College or University systems vulnerable to viruses, malware, zombies and or Trojans. If you are in doubt, you should contact the St Peter’s IT Department.

If sending large or multiple attachments exceeding 2MB, employees are advised to use the University OxFile service https://oxfile.ox.ac.uk. If access to OxFile does not exist, email may be used.

Cloud Services

You must obtain explicit authorisation from the IT Manager for the storing, exchanging or synching of confidential information in order to ensure that any such activity is secure. The University provides its own cloud services, OxFile (https://oxfile.ox.ac.uk/) and Nexus365 OneDrive storage (https://unioxfordnexus-my.sharepoint.com/;) public data storage services should not be used for personal or confidential information.

Hard copies

When sending confidential data by fax, you must ensure you use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

When sending confidential documents by post, whether internal or external post, you must ensure that the envelope is sealed securely, marked ‘Private and Confidential’, and addressed correctly. Recorded delivery must be used for confidential documents sent by external post.

9 Storage

Confidential data should be stored in the SPC file server, Zinc, and not on local hard drives, unless encrypted.

10 Access

To access the SPC file server, Zinc, you must obtain explicit authorisation from the IT Manager.

Having access to a shared drive does not imply that you have permission to view all the folders/files on that drive. You should view only the information you need to carry out your work.

Passwords must not be shared (except where specifically authorised by line management) or easy to guess.

11 Remote Access

Only trusted machines, not public kiosk machines, should be used to connect to the University network remotely.

Home computers used for remote access must be protected by a firewall, anti-virus software and by the installation of security updates.

12 Copying and working off-site

Confidential College data should be stored in the SPC file server, Zinc, and not on local hard drives.

Confidential data must not be copied from the SPC file server, Zinc, unless explicitly authorised the Bursar.

To avoid the risks of taking copies of confidential information off-site, you should as far as possible use remote access facilities to look at confidential information held on University systems.

Confidential data should be downloaded from a secure system (e.g. OSS, Oracle Financials, DARS) only when strictly necessary, and securely deleted after use.

You should ensure that any copies you make of confidential data are the minimum required and that they are deleted or destroyed when no longer needed.

13 Backup

Any critical files must be backed up via TSM (Tivoli Storage Manager, the University back up system). No further backups of files should normally be taken. For further information, please see http://help.it.ox.ac.uk/hfs/index

Before confidential data are encrypted, you must ensure that any critical data is securely backed-up.

You must ensure that mobile devices containing back-up copies of critical data are securely stored (see section 15 below on physical security).

14 Disposal

When disposing of surplus or obsolete mobile devices containing confidential data, you must ensure that any confidential data is removed permanently from the device (deleting the visible files is not sufficient).

You must remove any files or papers before disposing of old office furniture.

Confidential documents must be shredded when no longer needed.

When recycling old IT equipment, the hard drives must be removed and disposed of in an appropriate fashion ie crushing.

15 Physical Security and Hardware

You must lock your workstation, laptop or tablet when leaving your desk and log out when leaving for the day. Mobiles must be password protected.

Confidential data must be stored in a locked cupboard, cabinet or drawer. If this is not possible, you must lock the room when it is unoccupied for any significant length of time.

Keys to cupboards, drawers or cabinets must not be left on open display when the room is unoccupied.

When travelling with a mobile device, you must take reasonable care to reduce the risk of loss or theft.

You should not read confidential data in areas where others can easily view it.

Employees must not move or modify any hardware without the consent of the IT Department.

No non-University and non-College equipment may be attached to the network without consent of the IT Department. Hardware includes, but is not limited to monitors, base units, USB sticks and external hard drives. PDA devices such as mobile phones, tablet devices, eReaders are permitted.

All equipment must be treated with due care and attention and maintained in a condition and environment conducive to good working order and long life. Any fault, loss or damage must be immediately reported to the IT Department.

16 Software

College staff must not download software onto a College machine without obtaining authorisation from the IT Manager. Fellows must take care to ensure that any software downloaded to their machines must be from a trusted source.

The College computers will be set up by the IT Department and should not be altered by the user in any circumstances. Under no circumstances may you load any software without the approval of the IT Department. This includes software or other downloads from the internet.

Software issued by the College and / or the University for your use is licensed to the College and / or the University and is protected by copyright law. It is illegal to make copies of this software without the consent of the licence-holder. You should, therefore, not make copies of or distribute software without authorisation from the IT Department.

If you receive an `.exe' or `.dmg' file, you should not run it before informing the IT Department. Take care when decompressing zip files in case they contain an executable '.exe' file.

17 Passwords

In order to access software programmes you will be given a College/University user name and password by the Oxford University IT Services/IT Department. These are personal to you and should not be written down where they may be seen by colleagues or visitors.

While logged onto the College's system, you are responsible for all actions undertaken with your username and password. You should ensure that you do not leave the computer unattended while logged on.

You must not disclose any information relating to the College's system, which may make it vulnerable to a third party.

From time to time, you will be asked to give your password to another member of College or University staff, generally a member of the IT Department. You should not divulge passwords to anyone without the permission, where relevant, of your line manager. If you are in doubt, you should immediately ask for your password to be changed. Leaving notes detailing your user name and or password may constitute a disciplinary offence. When necessary, passwords should be communicated by text, and the text subsequently deleted.

If you require further network access beyond that currently authorised, you should contact your Manager who will authorise the IT Department to extend your access.

If you believe that another employee may have learnt your user name and password, you should change it immediately. The College and or the University will require you to change your password for the various systems at least once a year.

When changing your password, you should not use words or numbers, which contain personal data such as date of birth, or easily guessable words or numbers.

Disclosure of your user name and password to another user, or if you use another user's name and password, may be treated as a disciplinary offence, which may lead to disciplinary action.

18 Reporting

Suspected or actual security incidents e.g. the theft or loss of a mobile device, a virus attack, should be reported immediately to the Bursar and the IT Manager.

St. Peter’s College shall keep a record of all security incidents and follow the University’s advice for the escalation and reporting of such incidents. Incidents and breaches involving personal data shall be reported to the University’s Data Protection Team (data.protection@admin.ox.ac.uk) by the IT Manager and to the college’s DPO.

19 Enforcement

Any failure to comply with this policy may result in disciplinary action.

ANNEX A

University Supporting Policies

http://www.it.ox.ac.uk/infosec/

A comprehensive set of policy documents, regulations and guidance, within which the St. Peter's College's own Information Security Policy is framed.

https://www.it.ox.ac.uk/rules Regulations and Policies applying to all users of University ICT facilities. These apply to all staff, University and non-University library members and other relevant parties, including visitors and contractors. Students have to agree to these regulations and policies in order to activate their accounts on joining the University.

College Supporting Guidelines and Policies

Information Security Policy

- User Management Policy
- Physical and Environmental Security Policy
- Mobile Devices Policy
- Incident Response Policy
- Acceptable Use Policy
- Password Setting Policy

Information Security Policy/Payment Card Industry Data Security Standards (PCI DSS)

- Credit Card Handling Policy

ANNEX B

Examples of confidential information

The following list consists of generic examples and is for the purpose of illustration only.

Examples of Personal data[1]

1. Any set of data that could be used for fraud or identity theft, including but not limited to bank account or credit card details, national insurance number, passport number, home address, date of birth.

2. Data relating to an individual's application for a job, performance in a job interview, work performance, promotion or disciplinary record

3. Data relating to a student's academic performance or disciplinary record

4. Data relating to an individual's personal or family life e.g. their interests, hobbies, relationships

5. Any sensitive personal data, as defined in the GDPR ie information relating to:
   - health (mental or physical),including disability
   - ethnicity or race
   - sexual life
   - preferred gender identification
   - trade union membership
   - political opinions
   - religious beliefs
   - commission or alleged commission of a criminal offences
   - criminal proceedings

Examples of Business information

1. Information provided to the College on the understanding that it is confidential, whether explicit or assumed

2. Information the disclosure of which would disadvantage the University's position in negotiations, whether commercial or otherwise

3. Reorganisation or restructuring proposals that would have a significant impact on individuals, prior to a decision being announced

4. Exam questions before the examination takes place

5. Security arrangements for buildings or for high profile visitors or events

6. Papers discussing proposed changes to policies or procedures on high profile or sensitive issues, before the changes are announced

[1] Any recorded information, hard copy or electronic, which identifies a living individual e.g. name, e-mail address, reference, CV, photograph.