ST PETER'S COLLEGE
UNIVERSITY OF OXFORD

Information Security Policy

Contents

Executive Summary

St Peter's College's computer and information systems underpin the activities of the College. 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 it 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.

- The aim of this policy is 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 complies with this policy and all other University policies and procedures relating to information security;
- St Peter's 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 shall ensure that all users receive appropriate training in information security.

Core Procedures and Practices - digital

- College business must be conducted within the College's IT environment;
- Personal email accounts must not be used for College or University business;
- Mobile devices used to handle College information or files- laptops, tablets, smartphones, - must be appropriately secured with passcodes or biometric access. If they cannot be secured, they must not be used to handle College information;
- Memory sticks must be used only if there is no secure alternative and encrypted where possible;
- Email is not a secure form of communication. Users wishing to send confidential information should consider using more secure methods, or at least should minimise the amount of information sent this way. Where no suitable alternative to email exists, appropriate safeguards should be taken, such as file encryption or password protection of documents.
  See IT Services Securing Email http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/email-and-exchange-information#d.en.111095;
- Confidential information should not be stored in email 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 College network;
- Confidential information should be stored only on College servers or University of Oxford provided facilities such as OneDrive;
- Confidential information should be downloaded from secure University systems (e.g. eVision, Oracle Financials, DARS) only when strictly necessary and deleted after use;
- Passwords must not be shared (except where specifically authorised by line management) and must meet the password policy below;
- Home computers used to access University systems must be kept secure through firewalls, antivirus 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 College's DPO (Data Protection Officer);
- Only JICTS may dispose of redundant or surplus IT equipment so that our information can be kept secure;
- Appropriate physical measures must be taken to prevent the theft, loss or inadvertent exposure of confidential data. Lock computer screens when not at your desk, do not read confidential information in a public place where it can be viewed by others;
- Any security incidents or data breaches must be reported promptly to the Bursar who keeps a record in the GDPR Breaches Register.

Core Procedures and Practices – hard copy

- Appropriate physical measures must be taken to prevent the theft, loss or inadvertent exposure of confidential data. Lock away hard copy confidential documents, do not read confidential information in a public place where it can be viewed by others;
- Envelopes containing confidential documents must be sealed securely and addressed correctly and, in the case of external mail, sent by recorded delivery;
- Only the Facilities Manager may dispose of filing cabinets so that their contents can be appropriately protected.

Policy Objectives

Section 1 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 policies reside. **Annex A** provides a list of all other policies and procedures that support this policy.

Section 2 Scope
This policy is applicable to and will be communicated to all staff, members and other relevant parties who use St Peter's College IT systems and services. It covers, but is not limited to, any systems or data attached to the College's computer or telephone networks, any systems supplied by the College, any communications sent to or from the College and any data owned either by the University or the College held on systems external to the College's network.

Section 3 Roles and responsibilities
The Bursar is ultimately responsible for the maintenance of this policy and for its implementation within St Peter's College.

The IT and Website Committee is responsible for reviewing this policy annually on behalf of the Governing Body, with any significant changes to be taken to Governing Body for approval. The Committee will provide direction and support and promote information security through appropriate commitment and adequate resourcing.

The JICTS Consortium, of which St Peter's is a member, 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 with which 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 Head of JICTS.

IT security incidents should be reported to JICTS who will escalate as necessary. Data incidents and breaches should be reported to the DPO cbryan@grcilaw.com who will advise and escalate as necessary, and in certain cases report them to the Information Commissioner's Office (ICO).

Detailed Procedures and Practices

This section is directed at users and sets out the procedures and practices you need to follow in order to implement the objectives identified above, particularly in relation to the protection of confidential information.

Section 4 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 General Data Protection Regulation (GDPR), you should assume that all personal data is confidential. Personal data is any data that identifies a living individual such as CVs, email addresses, references, job or course applications, home contact details, etc.

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

Section 5 Use of mobile devices

The use of mobile devices (laptops, encrypted USB sticks, smartphones, 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 and ensure the latest version of software and operating systems are used. 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, especially that taken off our estate, and especially laptops, must be encrypted, secured by a password and/or biometrically and should not be left unattended at any time. In the event of any loss or theft, you are to inform JICTS immediately.

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

Should you receive a file in a 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 JICTS who will conduct a virus check and give you confirmation that it is safe to use.

Encryption of laptops and encrypted USB memory sticks
All devices that might be used to hold sensitive or confidential data must be encrypted. The College encrypts its computers using the Sophos cloud-managed encryption tools. Portable/removable storage media such as USB drives holding sensitive or confidential data must employ software or hardware encryption. These work like normal USB devices, but require a password to access data and are available through the College IT department. Sophos is installed on all College-managed computers.; advice on how to make college-owned devices more secure is available from JICTS. Some devices may have additional 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 site (https://www.it.ox.ac.uk/work-remotely#preparingtoworkremotely.). If this cannot be done, you must not use the device to hold or transmit confidential data.

Section 6 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://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002 for further details.

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 with due authorisation. Distributing data to third parties inappropriately could constitute gross misconduct potentially resulting in summary dismissal.

Confidential information should not be left on display on an unattended workstation.

Section 7 Email

Email 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. First consider communicating confidential information by a more secure method. If a suitable alternative is not available, you should consider encrypting the message and/or attachment.

Personal email accounts must not be used for College or University business. 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 'auto-complete' function. You should take particular care when selecting an address from a directory. Do not cc large numbers of people, use bcc instead.

If you receive confidential information inadvertently via email, you should delete it as soon as possible. Confidential information should not be stored in email 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.

Sending or receiving of illegal, defamatory or pornographic content 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. Contact JICTS with details of such emails.

Retention
Please delete unwanted emails or emails for which you can foresee no further use. Such deleted emails will remain on the system for a period of 90 days, and will be accessible from backup should you have deleted the email in error or, if an investigation into network abuse needs to be commenced. You may find it valuable to *archive* email inboxes prior to their deletion.

The College may access and monitor any or all areas of its computer network. Do not assume that any information held on the College or University system is private to you.

If you suspect that any of your email accounts have been compromised, you are to report this immediately to JICTS and, if applicable, your manager.

Employees should take all reasonable steps to ensure that emails they send to do not contain viruses or malware. Emails sent must not adversely affect the College's business operation, the safety of its members nor its public image. Emails sent beyond the College or University must contain the College email disclaimer, which can be obtained from the Communications Manager.

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, contact JICTS.

If sending large or multiple attachments exceeding 20MB, employees are advised to use the University OxFile service https://oxfile.ox.ac.uk/

Section 8 Storage
Data should be stored only in the SPC file servers and never on local hard drives or public cloud drives. The University provides its own cloud services, OxFile (https://oxfile.ox.ac.uk/) and Nexus365 OneDrive storage (https://help.it.ox.ac.uk/sharepoint); public cloud services should not be used for college information.

Section 9 Access and sharing files
To access the SPC file servers, you must obtain explicit authorisation from JICTS.

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.

Where individuals or teams frequently share data, this should be done through the use of a shared folder or drive on the SPC file servers rather than through email.

The College intranet exists to enable the sharing of committee papers with relevant groups of people, and to host frequently-used documents with specific sections of the College community.

Section 10 Remote Access
Only trusted machines, not public kiosk machines, should be used to connect to the University network remotely.

Where individually owned home computers are used for remote access they must be protected by a firewall, anti-virus software and by the installation of security updates. College files should be accessed only through the JICTS-supplied remote desktop access via the University VPN.

Section 11 Copying and working off-site
Confidential College data should be stored in the SPC file servers and never on local hard drives.

Confidential data must not be copied from the SPC file servers unless explicitly authorised by 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 engage with confidential information held on College or University systems.

Confidential data should be downloaded from a secure system (e.g. eVision, 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.

Section 12 Backup
Any critical files must be backed up via TSM (Tivoli Storage Manager, the University back up system). Files stored on College servers benefit from TSM back-\ups. 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 they are securely backed-up.

You must ensure that mobile devices containing back-up copies of critical data are securely stored (see Section 14 below on physical security).

Section 13 Disposal
Only JICTS may dispose of surplus or obsolete college-owned mobile devices and IT equipment. When selling or destroying your own hardware ensure factory settings have been restored.

Section 14 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 or biometrically protected.

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 Head of JICTS.

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

Section 15 Software

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

The College computers will be set up by JICTS and should not be materially altered by the user in any circumstances. Under no circumstances may you load any software without the approval of JICTS.

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 license-holder. You should, therefore, not make copies of or distribute software without authorisation from JICTS.

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

Section 16 Passwords

Your password is personal to you and should not be written down where it may be seen by colleagues or visitors. Leaving notes detailing your username and or password may constitute a disciplinary offence.

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.

You will never be asked share or divulge your passwords. If you are in doubt about who has your passwords you should immediately ask for your password to be changed and inform a member of JICTS.

If you believe that another employee may have learnt your username 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.

Ensure all passwords are at least 16 characters long. Never reuse passwords

MFA (Multi factor Authentication) and biometrics should both be used where possible.

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

Section 17 Reporting

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

St Peter's College will 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 JICTS and to the College's DPO.

Section 18 Physical Materials

Do not send confidential data by fax.

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.

Only the Facilities Manager may dispose of storage units. You must remove any files or papers before old office furniture is disposed of. Confidential documents must be shredded when no longer needed.

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.

Section 19 Enforcement
Any failure to comply with this policy may result in disciplinary action.

Annexe A University Supporting Policies

https://www.infosec.ox.ac.uk/

The above link gives 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

- User Management Policy
- Physical and Environmental Security Policy
- Mobile Devices Policy
- Incident Response Policy
- Acceptable Use Policy
- Information Security Policy/Payment Card Industry Data Security Standards (PCI DSS)
- Credit Card Handling Policy

Annexe 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. 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 College'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