2021

[redacted]

The following policy has been approved by 0 1

**NEW COLLEGE**
**INFORMATION SECURITY POLICY**
**Template v1.16.3 June. 2021**

[redacted]

***This page is intended as a digest of the attached intercollegiate policy on information security. For more detailed information, please refer to it.***

## Overview

Users of ICT within the University are subject in the first instance to the University ICTC regulations (2002) with subsequent amendments and available for review at: http://www.admin.ox.ac.uk/statutes/regulations/196

[redacted]

In support of this objective all users of data assets, whether they are manual or electronic, accept their roles and responsibilities in ensuring information is protected and are committed to:

- Treating information security seriously
- Maintaining an awareness of security issues
- Adhering to applicable security policies / following applicable guidance

Information relating to living individuals (such as may be found in Personnel, Payrolls, and Student Record Systems) should only be stored in the appropriate secure systems and is subject to legal protection. All users of the ICT system are obliged, under the terms of the UK GDPR, to ensure the appropriate security measures are in place to prevent any unauthorised access to personal data, whether this is on a workstation or on paper. Data also pertaining to research and other intellectual information and deemed sensitive by the College shall also have the same measures taken to safe guard it against unauthorized access and or theft.

## 3. Scope and definitions

The scope of this Information Security Policy extends to all New College's information and its operational activities including but not limited to:

- Records relating to pupils, students, alumni, staff, academic staff, visitors, conference guests and external contractors

[redacted]

as protecting physical paper copy of data wherever possible (e.g., clean desk policies).

- Meet legislative and contractual obligations
- Protect the College’s intellectual property rights
- Produce, maintain and test business continuity plans in regards to data backup and recovery
- Prohibit unauthorised use of the College’s information and systems
- Communicate this Information Security Policy to all persons potentially accessing data
- Provide information security training to all persons appropriate to the role
- Report any breaches of information security, actual or suspected to the Data Protection Coordinator  (DPO) in a timely manner

More detailed policy statements and guidance are provided in Section 7 of this Policy.

## 5. Risk Assessment and the Classification of Information

5.1 The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

5.2 The risk assessment should identify New College’s information assets; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to the College or University as a whole. In assessing risk, the College should consider the value of the asset, the threats to that asset and its vulnerability.

5.3 Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

5.4 Rules for the acceptable use of information assets should be identified, documented and implemented.

5.5 Information security risk assessments should be reviewed periodically and carried out as required during the operational delivery and maintenance of the College’s infrastructure, systems and processes.

5.6 Personal data must be handled in accordance with

[redacted]

## 6. Responsibilities

- The Governing Body is responsible for establishing the framework and to issue and review policy statements and procedures to support New College and the Universities Ordinances and Regulations with which members of the University/College must comply.
- Governing Body requires the head of each department in College to be accountable for implementing an appropriate level of security control for the information owned by that department and processed by persons accessing that data.
- Each person is accountable to their head of department for operating an appropriate level of security control over the information and systems he/she uses to perform his/her duties.
- Every user is required to obey all laws, including criminal, counter-terrorism, copyright, defamation and obscenity laws. College will render all reasonable assistance to enforcement officials for the investigation and prosecution of persons using technology in violation of any law.
- The DPO is responsible for coordinating the management of information security, maintaining this Information Security Policy and providing advice and guidance on its implementation.

It is noted that failure to adhere to this Policy may result in the

[redacted]

agreement.  College Officers or other relevant roles are responsible for completing leavers checklists and communicating those lists to appropriate sections of College.

7.1.6. The circumstances under which the College may monitor use of its ICT systems, and the levels of authorisation required for this to be done form part of the University's "Regulations Relating to the use of Information Technology Facilities".

[redacted]

7.3. **Servers** This policy specifically applies to server equipment owned and/or operated by New College, and to servers registered under any New College-administered network.

All internal servers deployed in the College must be administered by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes peer review and approval.

7.3.1. Physical servers must be housed in a location where physical access and the server environment (power, temperature, and humidity) can be controlled.

7.3.2. Servers should be backed up to offsite storage, such as the University HFS. (Refer to section 7.9 of this policy for fut.

7.4.3. All network activity should be logged in accordance with University IT Services policy. It is currently recommended that at least 60 days of logs be kept, and longer if possible to allow for any post-incident review. Logs must include identifiable data to enable traces back to specific events, computer systems, and specific users. Timestamps, MAC addresses, IP Addresses, and where possible usernames should be included in logging systems. These logs should be proactively monitored and reviewed as an early warning system for hacking or any other form of unauthorized activity.

Further information on network security and good practice can be found within the ITSS IS Toolkit http://www.it.ox.ac.uk/infosec/istoolkit/

### 7.5. **Email and Internet Use**

Policy for the use of electronic mail is covered by the University's ICTC regulations of 2002 (with subsequent amendments) and available at http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

Where email systems are hosted locally, it should be checked by the College’s ICT Services Department on a regular basis to ensure that it is being appropriately updated in regards to spam/virus filters. All email that passes through the email system shall be content checked and scanned for viruses and inappropriate content and cross checked against an internet “black list” of banned email addresses. For centrally hosted email by UNIVERSITY IT SERVICES (Office365), their information policy will take precedence.

7.5.1. College’s policy and procedure on staff use of email and the Internet should be included in the Staff Handbook.

7.5.2. Virus or other malware warnings should be forwarded to ICT staff for checking and distribution rather than sent to other users. Mass mailing users of address groups provided by the College is for work-related information only. This therefore excludes the use of the email system for advertising personal items for sale.

7.6. **Mobile Computing** (applies to any mobile hardware that is used to access College resources, whether the device is owned by the user or by the College.)

7.6.1. Persons with laptop computers and other mobile computing devices including mobile phones shall take all sensible and reasonable steps to protect them from damage, loss or theft. Such steps may include:

- Securing laptops and removable media whether in college or while travelling.
- Avoiding taking laptops into areas with a high risk of theft and locking such equipment in the boot of a vehicle when leaving it unattended

7.6.2. Persons using computing equipment in public places shall ensure that confidential information cannot be viewed by unauthorised persons (e.g. stations, airports, trains, etc.)

7.6.3. Use of external wireless access points shall be permitted provided that the firewall

have also been risk assessed and adhere to all other sections of this policy.

### 7.11. Homeworking

We support homeworking in appropriate circumstances either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular (full or part-time basis). In addition, occasional or permanent homeworking can, in certain circumstances, be a means of accommodating a disability and can be requested as a means of flexible working.

This policy sets out how we will deal with requests for homeworking, and conditions on which homeworking will be allowed. If you are allowed to work from home you must comply with this policy.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Please refer to Appendix 6 for Further Guidance on BYOD or Self-Managed Computing Devices

#### 7.11.1. Homeworking Arrangements

- There are a number of circumstances in which the ability to work from home on an occasional or temporary basis may be of benefit to you:
  a) when a dependant becomes unwell or arrangements for their care break down at short notice;
  b) when, despite being fit to work, travelling to the office is difficult (for example, due to recovery from an injury such as a broken leg);
  c) when public transport has been disrupted (for example by the weather or by a strike, that affects your travel arrangements); or
  d) when a quiet, uninterrupted work environment will assist in dealing with a backlog of administrative tasks or in writing reports to a deadline.
- In these circumstances working at home can be authorised by your head of department where, in their opinion:
  a) you have work that can be undertaken at home; and
  b) working at home is cost-effective and any increase in work that may be passed to your colleagues as a result is kept to a minimum.
- Your line manager may, where necessary, liaise with Human Resources to confirm arrangements.
- You may want to vary your working arrangements so that, either permanently or for a fixed period, you work from home for all or part of your working week. Any request to work from home must meet the needs of our organisational as well as your needs.
- College reserves the right to terminate homeworking arrangements, for example if your role changes such that homeworking is no longer suitable, subject to reasonable notice.

However, no updated version of the operating system or other software should be installed without a valid licence. This should leave a machine in a suitable state for disposal unless there is confidential or sensitive information on the disk. These disks require a secure wipe and/or physical destruction.

8.11.4. Reasonable efforts should be made to see if any other unit is able to make use of the equipment.
8.11.5. Equipment that has residual value may be sold, either to University/College members or outside bodies once all data has been completely removed from devices.
8.11.6. Where equipment has limited resale value, consideration should be given to whether it can be donated to any charitable or community project. If the equipment cannot be reused, then it should be recycled or disposed of in an environmentally-friendly manner.
8.11.7. Older CRT computer monitors and batteries will be disposed of in line with the University Policy UPS S5/11 on the disposal of hazardous waste (https://www1.admin.ox.ac.uk/safety/oxonly/upss511/hazardouswaste/)
8.11.8. Disks that have contained information classed as confidential or sensitive must be secure wiped using a tool such as PGP or DBAN or physically destroyed.

## 9. Data Breach/Loss & Incident Management

We are obliged under data protection law to report personal data breaches to the ICO (or, in the case of a personal data breach effecting individuals outside the UK, the relevant supervisory authority).

New College has appointed Simon Buchanan of ClearComm as Data Protection Officer (DPO). Christopher Thompson, ICT Director of New College is appointed internally as Data Protection Coordinator (DPC) and will manage our relationship with the DPO.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate or resolve the matter yourself. Please inform the DPC, immediately. You must also preserve all evidence relating to the potential personal data breach. Failure to comply with this policy may result in disciplinary action being taken against you.

### 9.1 Key Information

9.11.4. We must make our formal notification to the ICO (or relevant supervisory authority) within 72 hours of becoming aware of a breach. It is therefore crucial that you notify the DPC immediately so that we are able to comply with the law.
9.11.5. We may also need to inform the individual(s) whose data has been subject to the breach. Our DPO shall make the final determination in respect of any notifications to individuals. You are not permitted to notify individuals without prior consultation with or instruction from the DPC.
9.11.6. Regardless of whether we are required to make a notification to the ICO or individuals, all personal data breaches must be notified to our DPO via the DPC who shall maintain a record of the incidents.
9.11.7. We shall document, with your mandatory cooperation details of all breaches, their effects and the remedial action taken. We shall investigate whether or not each breach has occurred as a result of human error or a systemic issue and see how a recurrence can be prevented, whether this is through better processes, further training or other corrective steps. Failing to notify a breach when required to do so can result in New College incurring a significant fine and publicity of the failure may cause irreparable reputation damage. Please note that failure to abide by our policies and procedures may result in disciplinary

action.

9.12. **How to Recognize a Personal Data Breach**

9.12.4. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data whether unintentional or deliberate.

9.12.5. Whenever any personal data is lost, destroyed, corrupted or disclosed, a personal data breach will have occurred. This includes circumstances where someone accesses the data or passes it on without proper authorisation; or if i.e. that you become aware of the breach and not the time at which our DPO or the DPC is made aware.

9.14.5. Notification must be made notwithstanding whether or not we are in possession of full details of the breach, damage caused or individuals affected.

9.14.6. In the event that we are not able to make our notification within 72 hours we must give notification immediately thereafter and give reasons for our delay.

### 9.15. Your Obligation

9.15.4. On notifying the DPC who shall notify our DPO of the breach identified, you must assist in providing information as above, to the best of your knowledge. If you were not the individual to identify the breach but you are able to assist in providing relevant information you must cooperate in providing this information so that we are able to make our notification promptly and in any event within the time limit.

9.15.5. When reporting a breach, we must provide:

-

5. **Configure devices and computers securely**- Keep software up to date and configure your security.
6. **Use Anti-Virus**- Anti-virus software protects your computer from software viruses, and prevents you from accidentally passing them to people you work with.
7. **Security for mobile phones and tablets**- easily lost, broken and stolen. Make sure you backup, lock, configure “find my device”, and enable remote wipe.
8. **Social Media**- be careful what you post - posts could reveal information about yourself that could be used to your disadvantage or contravene your contract of employment. Also be aware that downloads could contain malware.
9. **Protect from theft, loss or breakage**- Don’t make it easy for your devices to be stolen, or to lose our valuaen, or i5(ha)3