Imperial College
London

Imperial College

Information Security Policy

Doc. Ref.	: Information Security Policy
Version	: 7.0
Status	: Approved
Date	: 29/06/2022
Approved by	: The Information Governance Steering Group
Review by	: 29/07/2023

1. OBJECTIVE

1.1 Information plays a fundamental role in supporting all activities of the College. Properly securing all information that College processes is essential to the success of its academic and administrative activities. This is to be achieved through managing the three essential attributes of information security: confidentiality, integrity and availability, which are the vital building blocks for safeguarding College's information.

1.2 The objectives of this policy are to:

1.2.1 enable adequate protection of all of the College's information assets against loss, misuse or abuse;

1.2.2 make all users aware of this policy and all associated policies, codes of practice and guidelines;

1.2.3 make all users aware of the relevant UK and European Community legislation, and their responsibilities regarding these;

1.2.4 create an awareness that appropriate security measures must be implemented across the College as part of the effective operation and support of information security;

1.2.5 make all users understand their responsibilities for protecting the confidentiality, integrity and availability of the data they handle.

1.3 This Policy should be read in conjunction with the College's Data Protection Policy and associated Codes of Practice, which provide more detailed guidance on protecting personal data.

The codes of practice linked to the policy are:

Reference	Title
IS_C01	Hardware and Software Asset Management
IS_C02	Electronic Messaging
IS_C03	Inspection of Electronic Communications and Data
IS_C04	Account Security Management

2. SCOPE

2.1 All College staff, students and other authorised third parties including guests to College, who may have access to information held by or on behalf of the College, must adhere to the College's Information Security Policy and its associated Codes of Practice. The scope of the policy covers their use of College-owned/leased/rented and on-loan facilities, and all non-College systems, owned/leased/rented/on-loan, when connected to the College network directly or indirectly, to all College-owned/licensed data and software, be they on College or on non-College systems, and to all data and software provided to College by sponsors or external agencies.

2.2 As stated in paragraph 2.1 of the Information Governance Framework, the policy applies to all data held by the College or on behalf of the College whether in electronic or physical format including:

- electronic data stored on and processed by fixed and portable computers and storage devices;

- data transmitted on networks;
- information sent by fax or similar transfer methods;
- all paper records;
- microfiche, visual and photographic materials including slides and CCTV; spoken, including face-to-face, voicemail and recorded conversation.

2.3 As stated in paragraph 2.3 of the Information Governance Framework, the following is the classification template which should be used for all College data; please see College's Data Protection Policy to find out more about how to protect data in respective categories:

2.3.1. Confidential Data:

a. Sensitive Personal Data: defined as the Special Categories of Data in Article 8 of the General Data Protection Regulation – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. (This includes patient identifiable data for research purposes.) Additional protection measures are required.

b. Highly Sensitive Organisational Data: Data, which could cause the College damage or financial loss if exposed, data protected by confidentiality agreements, legally privileged information, etc.

2.3.2. Restricted Data:

a. Personal Data: As defined in Article 4 of the General Data Protection Regulation as any information related to a natural person which can be used to identify them – special measures of protection is required.

b. Sensitive organisational data includes commercially sensitive planning / administrative or research data, etc. – protection measures are required.

2.3.3. Unrestricted Data:

a. Non-personal data (Organisational data)

b. Non-sensitive organisational data is data pertaining to College which may or may not be published by default, but may be disclosed via freedom of information requests subject to legal advice.

2.4 The policy applies throughout the lifecycle of all information from creation, storage, and use to disposal.

2.5 Although the use of social media resources by College members is unrestricted and not centrally moderated, the College requires its members to ensure they respect this policy and cause no damage to the College's reputation. For further information, refer to College's web guides on Social Media and Collaboration

Policy.

3. RESPONSIBILITIES

The key roles and responsibilities at College with respect to information governance are set out in the College's Information Governance Policy Framework (see section [4]). Of particular importance for compliance with this policy are:

3.1 Heads of Department

Head of Department are responsible that staff, students and other authorised individuals within their department or division are informed, and comply with this policy, particularly section 11: Conditions of Use of IT Resources, and associated Codes of Practice. They are also responsible that all information assets held by their departments or divisions are included in the College's Information Asset Register and an Information Asset Owner is assigned for every information asset.

3.2 Staff, students and authorised third parties

All College staff, students and authorised third parties must adhere to this policy and associated Codes of Practice. Compliance with the policy forms part of the Core Terms and Conditions of Service for College staff and forms part of the Regulations for Students. Section 11 of this policy, "Conditions of Use of IT Resources (Acceptable Use Policy)" is displayed and must be accepted by all staff and students before they can start using their College user name. Any actual, or suspected, information security incidents (such as accidental exposure or loss, unauthorised access, computer virus, malicious software) must be reported to the ICT's Service Desk immediately. Concerned individuals may contact any senior members of ICT or College directly. (See section 7.1 for their contact details.)

3.3 Chief Information Officer

The Chief Information Officer is responsible for overseeing ICT's resources to manage day-to-day information security activities. The Chief Information Officer may decide to audit systems to identify and mitigate risks, or to make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

4. COMPLIANCE WITH LEGISLATION

4.1 The College has an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular importance in this respect are the Computer Misuse Act 1990, The Regulation of Investigatory Powers Act 2000, the UK General Data Protection Regulation , Data Protection Act 2018, and "Prevent Duty Guidance" as directed by the Counter-Terrorism and Security Act 2015.

4.2 The requirement for compliance devolves to all users, who may be held personally responsible for any breach of the legislation. Failure of an individual student or member of staff to comply with this policy, or with any legislation, may lead to the instigation of the relevant disciplinary procedures as set out in the College's employment terms and condition and staff policies and the College Regulations for students. Failure of a contractor to comply could lead to the termination of a contract. In certain circumstances, legal action may be taken.

5. DATA ASSET REGISTRATION TOOL

5.1 The College's Information Asset Register and the Data Privacy Impact Assessment are described in the Data Asset Registration Tool Code of Practice.

6. MONITORING ELECTRONIC COMMUNICATIONS

6.1 In accordance with the "Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000", made under the "Regulation of Investigatory Powers Act 2000" (RIPA) 2000, the College will exercise its right to intercept and monitor electronic communications received by and sent from the College for the purposes permitted under those Regulations. The purposes cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to the system, e.g. hacking and denial of service attacks, ensuring the effectiveness of its operations and compliance with College policies and regulations. The monitoring process will be carried out in accordance with "Code of Practice 3: Inspection of Electronic Communications and Data".

7. INFORMATION SECURITY INCIDENTS

7.1 Anyone suspecting that there has been, or is likely to be an information security incident, such as a breach of confidentiality, availability, integrity of information, or misuse of an information asset, should inform the ICT's Service Desk immediately. You may also contact any senior members of ICT or College directly if you prefer to do so. (Refer to these locations for contact details: http://www.imperial.ac.uk/admin-services/ict/about-ict/leadership-organisational-structure/ and http://www.imperial.ac.uk/admin-services/secretariat/information-for-staff/college-contact-lists/principal-officers-and-their-assistants/) The Provost or, if not available, the Chief Information Officer, has the authority to take whatever action is deemed necessary to protect the College against breaches of security.

If the incident involves accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, you must report it immediately by completing a notification of data security breach and sending it to: 365-dataprotectionoffice@groups.imperial.ac.uk.

If the incident involves cardholder data (CHD) or cardholder data environment (CDE) as described in the College's Payment Card Industry Data Security Standards (PCI DSS) requirements, use the PCI DSS Incident Response procedure to report it.

7.2 In the event of a suspected or actual information security incident or an unacceptable network event, the Chief Information Officer may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network.

7.3 Failure to report an information security incident or data breach immediately may lead to disciplinary action being taken. If you are in any doubt regarding whether to report an incident, you should seek advice from ICT or the College's

Data Protection Officer.

8. SECURITY EDUCATION AND TRAINING

8.1 New users of IT facilities, staff, students and approved third parties, should be instructed on the College policies and Codes of Practice relating to information security. They should also be given training on the procedures relating to the security requirements of the particular work they are to undertake and on the correct use of the College's IT assets in general before access to IT services is granted. It is the responsibility of managers that their staff are suitably trained, and to maintain training records. They should be made aware of this policy including the reporting procedures in section 7.

8.2 All new staff of the College must complete the Information Security Awareness training and the Data Protection Awareness training, which are included within Imperial College Essentials. Staff are also strongly advised to attend the IT security inductions when joining the College, and must be aware of the latest ICT security advice.

9. SECURITY CONSIDERATIONS FOR EMPLOYMENT

9.1 Security roles and responsibilities, as laid down in this policy and related Codes of Practice, should be included in job descriptions, where appropriate. These should include any general responsibilities for implementing the security policy as well as any specific responsibilities for the protection of assets, or for the execution of particular security processes or activities.

9.2 Applications for employment or changes of role may require screening based on the Pre-employment Checks section of HR's Recruitment and Selection Procedure.

9.3 Agency staff and approved third party users of College information systems will be required to sign a confidentiality or non-disclosure agreement as part of their contract as well as a data sharing agreement where they will have access to College personal data.

10. PROTECTING SPECIAL CATEGORY DATA

10.1 It is essential that the College protects special category data with enhanced security measures.

10.2 Special category data must not be stored on or communicated through services which are not provided by the College such as personal email (Gmail, Hotmail etc…) or web-based 'cloud' storage services (e.g. Google Apps, Dropbox).

10.3 For guidance on protecting special category data, refer to College's Data Protection Policy, Handling of Special Category Data Code of Practice and the Be Secure pages on the College website.

10.4 Databases and computers containing special category data must be encrypted and require users to input credentials to access the data. Where possible, data should be anonymised or pseudonymised to remove personal identifiers, especially where patient/participant identifiable data is considered.

10.5 All College devices must be securely wiped before being disposed of. More information is available from ICT on how to dispose of hardware.

10.6 Data files must be encrypted both at rest and in transit. For more information, refer to ICT's Encrypt Sensitive Information pages.

11. CONDITIONS OF USE OF IT RESOURCES (ACCEPTABLE USE POLICY)

As a student, staff member or an authorised third party accessing and using College IT resources I agree and accept that:

11.1 College IT resources are all hardware, software, services and resources made available for the College business. They include all computer networks, wired or wireless, computers, printers, mobile devices, storage, audio visual systems, and associated information services including Cloud services.

11.2 I understand and abide by the advice provided in the Be Secure web pages and must enrol and complete the College's Information Security Awareness and Data Protection Awareness training.

11.3 My use of College IT resources and access non-College IT resources must be for the purpose of College research, teaching, coursework, associated administration or other authorised use. No private commercial work is permitted without prior authorisation.

11.4 College business should be conducted only on information services provided by the College. Using non-College services to carry out College business puts College data at risk and therefore is not allowed except with sufficient justification. For example, Qualtrics should be used instead of SurveyMonkey, SharePoint or OneDrive instead of Dropbox, and College Email instead of Gmail, Hotmail, etc.

11.5 Reasonable personal use of College IT resources is permitted provided such use does not disrupt the conduct of College business or other users. Recreational use of the Halls of Residence network is also permitted, subject to these conditions.

11.6 It is not permitted to connect active network devices such as network switches, hubs, wireless access points and routers to the College network. All IP addresses will be allocated and administered only by ICT.

11.7 I may not grant access to College computing services to non-College staff or students except where expressly permitted to do so in writing.

11.8 When using College IT resources I must comply with the College's Information Security Policy including this Acceptable Use Policy, JANET Acceptable Use Policy, and all relevant statutory and other provisions, regulations, rules and codes of practice. Specifically, but not exclusively, **I must**:

11.8.1 not disclose to others my College password and must understand and abide by "Code of Practice 4: Passwords";

11.8.2 not access or attempt to access IT resources at College or elsewhere for which permission has not been granted or facilitate such unauthorised access by others;

11.8.3 not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any IT resources at the College or elsewhere, e.g. port scanning;

11.8.4 not display, store, receive or transmit images or text which could be considered offensive or which is likely to bring the College into disrepute, e.g. material of a pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory, illegal, discriminatory, or terrorist nature;

11.8.5 not forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' email, must not impersonate others in electronic communication and generate junk or offensive communications and must understand and abide by “Code of Practice 2: Electronic Messaging”;

11.8.6 ensure all mobile devices I use to access College resources are encrypted by an appropriate encryption software, and pin or password protected;

11.8.7 respect the copyright of all material and software made available by the College and third parties and not use, download, copy, store or supply copyrighted materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the College. Staff and students are strictly prohibited from downloading software from unauthorised sources. Please liaise with ICT should you require a licence for software packages to ensure you can gain legal access to software;

11.8.8 when holding data about living individuals, abide by the College’s Data Protection Policy, to process information (that is, collect, use, share and dispose of) in accordance with the Principles of the data protection legislation. Students must not keep personal data concerning individuals in connection with their academic studies/research without the express approval from their Head of Department;

11.8.9 when responsible for information assets as an identified Information Asset Owner, understand and abide by their responsibilities as defined in “Code of Practice 7: Data privacy impact assessment” under the Data Protection Policy;

11.8.10 be aware that all information assets created/owned/stored by the user on or connected to College IT resources may, in the instance of suspected wrong doing, be subjected to inspection by College or by statutory authorities. Should the information be encrypted the user shall be required to and must provide the decryption key;

11.8.11 establish what the terms of the licence are for any material and software which I use through any platform and must not breach such licences including those which relate to “walk-in” access to particular materials which should only be accessed in Imperial College Libraries.

11.8.12 not remove or disable any diagnostic and management software installed on College computers by ICT.

11.8.13 understand and abide by the Imperial College’s Payment Security and PCI DSS (Payment Card Industry Data Security Satandards) policies, if I am associated with the College’s Cardholder Data Environment (CDE), process card payments, or support the payment card technical infrastructure.

11.9 As provided by the “Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000”, made under the “Regulation of Investigatory Powers Act 2000” and “Prevent Duty Guidance” as directed by the "Counter-Terrorism and Security Act 2015" the College will intercept and monitor electronic communications for the purposes permitted under those Regulations in accordance with "Code of Practice 3: Inspection of Electronic Communications and Data".

11.10 In the event of a suspected or actual information security incident or an unacceptable network event, the Chief Information Officer may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network.

11.11 In the event of further examination required, ICT may take action to examine any systems on the College network by express permission from the College Secretary.

11.12 Other than as per any applicable statutory obligation, the College will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT resource provided and/or managed by the College.

11.13 Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data.

11.14 My name, address, photograph, status, e-mail name, login name, alias, College Identifier (CID) and other related information will be stored electronically for use for administrative and other purposes e.g. monitoring system usage. Where I have opted to use it for authentication, my biometric data, such as finger-print and face identification data, may also be stored on encrypted devices, and will only be used for authentication purposes.

11.15 These conditions apply to non-College owned equipment e.g. personal Laptops, home PCs when connected to the College network, directly and/or via the VPN, for the duration that the equipment is using the College network.

11.16 I will remove / wipe off all College licensed software and data installed / stored on my personal computer(s) immediately upon leaving the College.

11.17 Breach of these conditions may lead to College disciplinary procedures being invoked, with penalties which could include suspension from the use of all College IT resources for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the College and may involve civil or criminal action being taken against the user.

11.18 If you have any questions, contact ICT's Service Desk.

11.19 All guests using College IT facilities and/or the College internet connection must be known to a member of College as their sponsor. Sponsors must be able to identify and take responsibility for the actions of their individual guests. For further information regarding the setup of guest accounts, refer to ICT's Guest Accounts page.

Version History

Version/Status	Release Date	Comments
1.0/Approved	January 2013	Approved
2.0/Approved	March 2016	UK Legislation in paragraph 14 have been updated; “Prevent” act added.
2.1/Revised – In Review	April 2016	Comprehensive revision as per findings report of the Information Governance Audit in 2015. Reviewed by Prof Alan Boobis, Jes Silver (College Data Protection Officer), Dr John Shemilt (Director of ICT), Matthew Williams (Network and Security Manager), ICT Security Team
2.2/In Review	May 2016	Reviewed by ISSG, Mike Russell and revised accordingly
2.3/In Review	July 2016	Reviewed by John Neilson, College Secretary and Mike Russell, CIO
2.4/In Review	July 2016	Reviewed by IGSG.
3.0/Approved	November 2016	Published following Provost Board Approval
3.1/In Review	January 2018	Review by IGOG members
3.2/In Review	March 2018	Review by Jon Hancock, Head of Central Secretariat, Milena Radoycheva, Head of Legal Services, and Robert Scott, College DPO.
3.3/In Review	16 March 2018	Submitted to the Provost Board
4.0/Published	20 March 2018	Published following Provost Board approval
4.1/In Review	March 2019	Annual review carried out by Tim Rodgers and Okan Kibaroglu and Matthew Williams
5.0/Published	April 2019	After review by IGSG
5.1/In Review	May 2020	All references to IT Director replaced with Chief Information Officer. Additional clarification regarding software piracy added to 11.8.7.
5.2/In Review	July 2020	Moved CoP 1 related to DPIA to Data Protection Policy; new CoP 1 added “Hardware and Software Asset Management”. Contents of Paragraph 5 IAR and DPIA are moved to the Data Protection Policy.
5.3/In Review	Jan 2021	Reviewed by John Neilson, the College Secretary.
6.0/Published	Jan 2021	Confirmed to be published by John Neilson
6.1/In Review	June 2021	Multi Factor Authentication added
6.2/In Review	April 2022	2.3.1 - replaced current classification wording to new wording found in updated Information Governance Framework 4.1 amended reference / hyperlink of EU GDPR to the UK GDPR 5. Updated to reference DART 7.1 PCI DSS incident reporting statement added 8.2 changed word ‘should complete’ to ‘must complete’ as per Imperial Essential requirements 10 Amended to change ‘sensitive’ to ‘special category’ which is the legal terminology 11.8.13 PCI DSS policies referred to as a requirement for those involved in PCI DSS processes
7.0/Published	29 June 2022	Reviewed and approved by the Information Governance Steering Group