Royal Holloway, University of London

Information Security

1. Introduction and Purpose

1.1 Royal Holloway subscribes to sound corporate governance principles, one of which is the use and application of Policies and Governance Standards which define and articulate practices, boundaries, and expectations within which the College will operate.

1.2 This policy supports the College's Information Risk Appetite and defines the minimum requirements to be implemented which relate to the control and authorized use of the College's information and assets.

1.3 Information Risk is defined as the risk of accidental or intentional unauthorised use, modification, disclosure or destruction of information resources, which would compromise the confidentiality, integrity and availability of information and which could potentially harm the College.

1.4 The purpose of the Information Security Policy is to ensure that the College's information and communications technology systems are consistently protected from compromise.

1.5 Information Security Policies and corresponding Standards and Procedures are the primary means by which the required College baseline security requirements are translated into specific, measurable, and auditable goals and objectives.

1.6 The objectives of the controls are to ensure that there is a comprehensive set of accessible policies which is reviewed regularly and approved by an appropriate governance committee.

1.7 Failure to maintain a suitable Information Security policy and compliance framework can lead to:

- 1.7.1 Operational outages and damage caused by unavailability, inaccessibility or corruption of Royal Holloway information assets.
- 1.7.2 Higher operating costs or financial loss or loss of earning potential to the College.
- 1.7.3 Decrease in College funding, damage the College's reputation and its relationship with its stakeholders (including research funders and prospective students and collaborators).
- 1.7.4 Impacts on research and academic standing.
- 1.7.5 The undermining of the management of the College and its operations.
- 1.7.6 Compliance fines and monetary penalties of the Information Commissioner's Office can reach up to 20 million euros or 4% of turnover.
- 1.7.7 A loss of trust and a breakdown in relationships within the College.
- 1.7.8 Damage and distress being caused to those who entrust Royal Holloway to look after their personal data.
- 1.7.9 Risk of fraud or misuse of compromised personal data.
- 1.7.10 Breach confidence of information provided by third parties.
- 1.7.11 Disadvantage the College in commercial or policy negotiations.
- 1.7.12 Prejudice a criminal investigation or enable criminal activity.
- 1.7.13 Breach contractual agreements.
- 1.7.14 Breach a duty of confidentiality or care.
- 1.7.15 Lawsuits, individual civil action for breaches of data protection can also be taken by individuals.

2. Scope

2.1 This policy applies to all users of Royal Holloway's computing resources, networks and data. Individuals covered by the policy include (but are not limited to) Royal Holloway, staff, students, alumni, guests or agents of the administration, external individuals (e.g. 'visiting fellows') and organisations accessing network services via Royal Holloway's computing facilities and networks.

2.2 Computing resources include all Royal Holloway owned, licensed, or managed hardware and software, and use of the Royal Holloway network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

2.3 This document defines the College's high-level Information Risk Policy and breaks this down into a further 11 specific policy areas, aligned to the international standard for Information Security Management Systems (ISMS), ISO27001. This document is intended to provide a high-level overview of the range of policies and where necessary it refers to more detailed policy documents which cover each area in greater detail.

3. Policy Statement

The following principles must be adhered to and guide the implementation of this policy.

3.1 Information is a valuable asset to the College and must be protected accordingly.

3.2 All formats of information, hard copy or electronic, structured, or unstructured, must be similarly protected.

3.3 Information must be protected throughout its lifecycle, which consist of creation, processing, transmission, storage, archiving retention and disposal.

3.4 Information must be protected regardless of its location (e.g., owned data centres, hosted premises, remote or outsourced sites, personally owned devices).

3.5 Protection should always be focused on information assets rather than simply on the hardware that is used to store or process them.

3.6 Information must be protected according to its:

3.6.1.1 Confidentiality

3.6.1.2 Integrity

3.6.1.3 Availability

3.7 Information risk control requirements for compliance with legislation, regulation and contracts that apply to the College must be defined, documented, and implemented in the relevant areas and policies.

3.8 Non-repudiation, the ability to prove an action or event has taken place and cannot be denied later, must be ensured where required.

3.9 Information assets must be protected from potential threats (potential source of an event with a likelihood of occurrence) that may exploit vulnerabilities (weakness in an information system, procedures, internal controls, implementation, or organization).

3.10 Ownership and accountability for protecting information assets must be clearly defined and accepted.

3.11 The College must take responsibility for the actions of its consultants, contractors, suppliers and third-party service providers in ensuring that they adhere to the same standards expected of its employees.

3.12 Cloud and outsourced services shall use robust and actionable contractual conditions to maintain the College's IT security standards in any software as a service, platform as a service or infrastructure as a service context.

3.13 Roles and areas of responsibility must be segregated to minimize opportunities for misuse, abuse of privileges and unauthorized or unintentional modification of information assets.

3.14 Appropriate contacts with relevant authorities must be maintained to enable relevant assistance with legal and security issues.

3.15 Appropriate contacts with special interest groups or other specialist security forums and professional associations must be maintained to maintain a current understanding of information security threats and best industry practice.

3.16 Information security must be addressed in project management, regardless of the type of the project.

3.17 There must be a comprehensive set of policies and controls structured to enable easy reference by all employees.

3.18 Policies and controls must be reviewed periodically, approved and signed off by an appropriate governing committee.

4. Human Resources Information Security

The purpose of the Human Resources Information Security category is to ensure that the College and its assets are protected from damage caused by employees, contractors, and other people with access to information assets:

4.1 To ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

4.2 To ensure that all employees, contractors, and third-party users are aware of information security threats and concerns, their responsibilities, and obligations, and are equipped to support organizational security policy in the course of their normal work.

4.3 To ensure that employees, contractors, and third-party users exit an organization or change employment in an orderly manner that does not put information at risk.

4.4 Human Resources Information Security Controls

The following high-level controls must be adhered to:

4.4.1 Proportionate background checks on candidates for employment must be carried out in line with relevant regulations and ethics before employment commence.

4.4.2 All in scope users accessing College information assets must receive appropriate information security awareness training.
4.4.3 All in scope users must return College information assets on termination or change of their employment, contract, or agreement.
4.4.4 The access rights of all users must be appropriate to role and therefore, Human Resources must ensure that Access Management are made aware of role changes that have Human Resources involvement.
4.4.5 The contractual agreements with employees and contractors shall state their and the College's responsibilities for information security.
4.4.6 There shall be a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.

5. Student Information Security Awareness

The purpose of the Student Information Security Awareness category is to ensure that the College and its assets are protected from damage caused by students with access to information assets:
5.1 To ensure that students understand their responsibilities and to reduce the risk of theft, fraud or misuse of College facilities and information assets and their own personal data.
5.2 To ensure that students are aware of information security threats and concerns, their responsibilities, and obligations, and are equipped to support organisational security policy during their studies.
5.3 To equip students with the skills and knowledge they require to remain safe and secure within digital environments for their studies and future employment.

5.4 Student Information Security Awareness Controls

The following high-level controls must be adhered to:
5.4.1 All students accessing College information assets must receive appropriate information security awareness training.
5.4.2 There shall be a formal and communicated disciplinary process in place to act against students who have committed an information security breach.

6. Information Asset Management

The purpose of the Asset Management category is to ensure that information assets are protected in a way which is appropriate to their business use and proportionate to business risk to:
6.1 To identify organizational assets and define appropriate protection responsibilities.
6.2 To ensure that information receives an appropriate level of protection, proportionate to the risk presented by loss of confidentiality, integrity, or availability.
6.3 To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

6.4 Information Asset Management Controls:

The following high-level controls must be adhered to:
6.4.1 All material information assets must be identified, documented, and have defined information owners.
6.4.2 Information owners must classify their information in a manner relative to the level of its value, sensitivity, and criticality as well as legal, regulatory, and business requirements.
6.4.3 Information must be appropriately labelled to indicate its classification level. Handling requirements based on classification level must be implemented throughout the information lifecycle.
6.4.4 Information assets shall be categorised, retained, stored, handled, and deleted according to legal and regulatory requirements as specified in the Information Classification and Handling Standard.

7. Access control

The purpose of the Access Control category is to define:
7.1 The correct use and management of information system access controls within the College.
7.2 Authorised access to information systems.
7.3 The measures to be applied to information assets to ensure the confidentiality, availability and integrity of those assets.
7.4 The policy governing the lifecycle of Access Control (including provisioning and de-provisioning processes).

7.5 The requirements for identifying users and their access rights to the College's information and information systems.

7.6 **Access controls:**

The following high-level controls must be adhered to:

7.6.1 User access will be granted on the principle of 'least privilege' and managed throughout their lifecycle to ensure appropriate access to the right resources at the right time.

7.6.2 Each account (system, user, service, application) must have a single identifiable owner who shall be held accountable for all actions performed by this account.

7.6.3 Access shall be granted appropriate to role.

7.6.4 Appropriate authentication mechanisms must be used to verify user identity.

7.6.5 Approval must be given before any access is provided.

8. Physical and environmental security

The purpose of this category is to protect the College and its assets using physical controls. The objectives of the controls are:

8.1 To prevent unauthorised physical access, damage and interference to the College's information and information systems.

8.2 To prevent loss, damage, theft or compromise of these assets and interruption to the College's activities.

8.3 **Physical and environmental controls:**

The following high-level controls must be adhered to:

8.3.1 The College's premises which hold information assets, and their supporting utilities must be protected against environmental and physical threats.

8.3.2 Physical access to information and information systems must be controlled to prevent unauthorised access.

8.3.3 Security perimeters shall be defined and used to protect areas that contain information processing facilities and either sensitive or critical information.

8.3.4 Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

8.3.5 Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

8.3.6 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

8.3.7 Security shall be applied to off-site assets considering the different risks of working outside the College's premises.

8.3.8 All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

8.3.9 Equipment shall be correctly maintained to ensure its continued availability and integrity.

8.3.10 Equipment, information, or software shall not be taken off-site without appropriate prior authorization.

8.3.11 Users shall ensure that unattended equipment has appropriate protection.

8.3.12 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

9. Operational security

The purpose of this category is to define the principles required to ensure the correct and secure operation and use of information processing facilities. This is done through effective design, operation, and monitoring of secure operational processes, through detecting and addressing any vulnerabilities to the College's systems and information, and through backing up data for restoration in the event of accidental or malicious damage:

9.1 To ensure correct and secure operations of information processing facilities.

9.2 To ensure that information and information processing facilities are protected from threats such as malware, software bugs, unauthorised software installations and exploitation of other technical vulnerabilities.

9.3 To protect against loss of data.

9.4 To record events and generate evidence.

9.5 To maintain the integrity of application system software and information.

9.6 To ensure the effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information.

9.7 **Operational Security Controls:**

The following high-level controls must be adhered to:

9.7.1 Operations Security procedures must be documented and maintained.

9.7.2 The College approved malware protection software must be installed, configured and maintained on all relevant systems.

9.7.3 Current copies of information assets must be stored securely and be accessible to recover information in the event of loss.

9.7.4 Systems holding or processing high value information must have appropriate logging or monitoring enabled, suitably qualified individuals will be given access to these logs as a preventative measure to identify patterns of misuse and / or events of concern.

9.7.5 Any changes to College's information systems must be managed and executed using an approved change management process.

9.7.6 Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations.

9.7.7 Critical systems should have an adequate capacity management process.

9.7.8 Access to production systems (privileged and other) should be in line with the documented access control and logging standards.

9.7.9 The clocks of all relevant information processing systems within the College domain shall be synchronised to a single reference time source.

9.7.10 All software installation should follow set guidelines and standards as described in the Acceptable Use of Information Technology policy.

10. Communications and Network Security

The purpose of the category is to define and enforce the guiding principles, policies and procedures required to ensure the secure design, management, and operation of the College's IT network. It defines measures to protect College networks from external threats (e.g., from public Internet) and from internal disruption:

10.1 To ensure the protection of information in networks and the protection of the supporting infrastructure.

10.2 To maintain the security of information transferred within the College and with any external entity.

10.3 To ensure the security of remote-working and the use of mobile devices.

10.4 **Communications and Network Security Controls:**

The following high-level controls must be adhered to:

10.4.1 Network controls must be implemented to protect information and to maintain the availability of network services including Remote-working, Mobile Devices and BYOD (Bring Your Own Devices).

10.4.2 Outbound electronic communications must be scanned, and controls implemented where there is a high risk of sensitive information leaving the organization without authorization.

10.4.3 Mobile devices with access to College's data must be physically protected and secured when being used, stored and / or transported.

11. System Acquisition, Development, and Maintenance

The purpose of the Systems Acquisition, Development and Maintenance category is to ensure that information security is an integral part of the design and implementation of all the College's information systems. When new systems or changes are implemented, security considerations must be an integral part of the development lifecycle. Security requirements must be identified and agreed prior to the development and/or implementation of information systems:

11.1 To ensure that security is an integral part of information systems.

11.2 To ensure that information security is designed and implemented within the development lifecycle.

11.3 To ensure the protection of data classified as sensitive or confidential used for testing.

11.4 To prevent errors, loss, unauthorized modification, or misuse of information in applications.

11.5 To maintain the security of application system software and information.

11.6 **System Acquisition, Development and Maintenance Controls:**

The following high-level controls must be adhered to:

11.6.1 Areas of the College acquiring and developing a new IT system must follow the relevant governance process to assess the information risks and define the required information risk controls and capacity requirements, with input from all relevant stakeholders.
11.6.2 Appropriate levels of change control must be applied to all types of IT system changes and only approved and accepted changes are to be implemented.
11.6.3 Controls must be implemented to restrict and manage access to source code of IT systems.
11.6.4 The production, development and testing environments must be segregated either logically or physically.
11.6.5 Sensitive, confidential and production data may not be used in a test system without effective obfuscation and/or access control arrangements.

12. Supplier Relationships

The purpose of the Supplier Relationships category is to ensure that services supplied by third parties do not compromise the College's Information Security:
12.1 To ensure protection of the College's assets that is accessible by suppliers.
12.2 To maintain an agreed level of information security in line with supplier agreements.

12.3 **High-Level Controls:**
The following high-level controls must be adhered to:
12.3.1 All software and IT hardware must be purchased from approved College suppliers and third parties.
12.3.2 All third parties must formally agree to adhere to the College Information Security Policy before exchange of any services.
12.3.3 The third-party adherence to the policy should be monitored by an accountable relationship owner within the College.
12.3.4 Any changes to the third-party risk profile must be re-evaluated.
12.3.5 Any changes to third-party services described in the agreements must be managed in accordance with an approved change process.
12.3.6 Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.
12.3.7 Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

13. Information Security Risk and Incident Management
The purpose of this category is to define the guiding principles, policies and procedures required to ensure that information security events and weaknesses associated with information systems are reported and dealt with in a manner that allows corrective action to be taken to minimize the impact to the College:
13.1 To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
13.2 To ensure a consistent and effective approach is applied to the management of information security incidents and risks.

13.3 **Information Security Risk and Incident Management Controls:**
The following high-level controls must be adhered to:
13.3.1 Incidents:
13.3.2 Information risk incident management function and processes must be established that ensures the reporting of incidents within set timelines.
13.3.3 Reported information risk incidents must be recorded, assessed, resolved, and disclosed, where applicable, within set timelines.
13.3.4 The severity level of the reported information risk incident must be assessed using defined criteria and appropriate action taken.
13.3.5 A post-incident review must be done, and remedial action must be taken to reduce the likelihood of the information risk incident recurring.
13.3.6 Employees authorised to conduct forensic investigations or monitoring may not conduct monitoring without an approval for interception. Interception must be limited to its stated purpose.
13.3.7 Procedures for handling intercepted data must protect the privacy of the communicating parties, as far as is consistent with the approved purpose.

13.3.8 The College shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

13.3.9 Risks:

13.3.10 Information owners must ensure that information risks are assessed, and risk tolerance and appetite levels must be defined.

13.3.11 Risks must be addressed through risk treatment options as per the Information Security Risk Assessment and Treatment Standard and treatment plans must be executed accordingly.

13.3.12 The residual risk must be determined and approved by the business area in conjunction with Integrated Operational Risk.

14. Continuity Management

The purpose of this category is to ensure that information security is not compromised as a result of interruptions to business caused by major failures or disasters, and to ensure that information processing services are resilient and resumed in a timely manner following an interruption:

14.1 Information security continuity should be embedded in the College's business continuity management systems.

14.2 To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

14.3 **Continuity Management Controls:**

The following high-level controls must be adhered to:

14.3.1 Business continuity plans must consider the impact of business process interruptions on information risk, must be documented, maintained, and tested.

14.3.2 IT disaster recovery processes must include information risk requirements.

14.3.3 The established and implemented information security continuity controls shall be verified at regular intervals to ensure that they are valid and effective during adverse situations.

14.3.4 Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

15. Logging and Monitoring

The purpose of this category is to ensure:

15.1 Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

15.2 Individuals must not have an expectation of privacy in anything they create, store, delete, send, or receive using the College's information technology resources. All information stored or communicated using the College's information systems, including electronic mail and instant messaging is the property of the College and is subject to the conditions of College's policies.

15.3 The College maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited.

15.4 The College reserves the right to examine College provided e-mail accounts, file directories, web access, telephonic and online chat conversations and other information stored on the College's computers. The specific content of any transactions may be viewed if there is a suspicion of improper use. E-mail content may be monitored through automated means.

15.5 Any E-mails you send or receive, and other electronic records may be subject to requests under the freedom of information or disclosure to enforcement agencies in connection with civil litigation or regulatory investigation.

15.6 Periodic review of Social Media sites will be performed for any mentions of the College within business or personal accounts.

16. Roles and Responsibilities

16.1 Compliance with this document is mandatory for all users of Royal Holloway Information Technology resources.

16.2 All staff shall be responsible for maintaining compliance with information processing procedures with the appropriate security policies, standards, and any other security requirements. Information owners shall regularly review the compliance within their area of responsibility.

16.3 The IT Services Department is responsible for the implementation of this policy and may enlist other departments to assist in the monitoring and maintenance of compliance with this policy.

16.4 Any enquiries or comments regarding this policy shall be submitted to the IT Services Team by sending an email to ITServiceDesk@rhul.ac.uk.

17. Related Documents

17.1 ISO/IEC 27001:2013 Information Security Standard; https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/

18. Monitoring and Compliance

18.1 If for any reason users are unable to comply with this policy or require use of technology which is outside its scope, this should be discussed with their line manager in the first instance (for staff) and then the IT Services team who can provide advice on escalation/exception routes.

18.2 Exceptions to any part of this document must be requested via email to the IT Services team. A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Chief Information Officer.

18.3 Exceptions to this policy must be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

19. Document Control Information

Policy Owner *(usually Director-level)*	Chief Information Officer
Approving Body	Executive Board
Approved on	19/10/2021
To be reviewed before	October 2023

Version History		
Version (newest to oldest)	Date of approval	Summary of changes
0.1	16/02/2021	First Draft
0.2	10/06/2021	Reformat to College standard, amended to remove references to pending standards
0.3	16/06/2021	Further amends based on internal feedback and submission to Information Technology Committee; draft submitted to Information Governance Committee for feedback
0.4	18/10/2021	Missing section 18 restored
0.5	21/06/2021	Amends based on Information Governance Committee Feedback including separation of HR and student information
0.6	03/08/2021	Proof reading changes prior to final internal circulation and submission to ITC
1.0	08/10/2021	First submission for approval at Information Technology Committee and Executive Board
1.0	19/10/2021	Executive Board Approval