1. Introduction and Purpose

1.1 The computing resources at Royal Holloway support the educational, instructional, research, administrative and voluntary activities of the college and the use of these resources is a privilege that is extended to members of the Royal Holloway community.

1.2 As a user of these services and facilities, you have access to valuable Royal Holloway resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to consistently behave in a responsible, ethical, equitable and legal manner.

1.3 In general terms, 'acceptable use' means respecting the rights of other computer users, the integrity of the college's physical facilities and all pertinent license and contractual agreements. Inappropriate use or behaviour exposes Royal Holloway to risks including malware attacks, the compromise of network systems and services, and legal issues.

1.4 Compliance with this policy is mandatory. If an individual is found to be in violation of the Acceptable Use Policy, the College may take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result action being undertaken under the Staff Disciplinary Policy and Procedure or the Student Conduct Regulations.

1.5 Individuals are subject to United Kingdom laws governing the many interactions that occur on the Internet. These policies and laws are subject to change as UK law develops and changes.

1.6 As a member of the Royal Holloway University of London community, the college provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet.

1.7 You are responsible for knowing the policies and standards of the College that apply to appropriate use of its technologies and resources.

1.8 You are responsible for exercising good judgment in the use of the College's technological and information resources.

1.9 As a representative of the Royal Holloway community, when representing the College you are expected to respect the good name of Royal Holloway in your electronic and online dealings with those outside the College.

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 organizations 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.

3. Policy Statement

3.1 Information Security Awareness

3.1.1 Royal Holloway is committed to establishing an information security-aware culture to help protect its information assets.

3.1.2 All new users must acknowledge and accept the Acceptable Use agreement before access to Royal Holloway systems is granted.

3.2 New Staff and students (Joiners)

3.2.1 All new staff must complete information security awareness training within an established training timeline and regularly thereafter.

3.2.2 Information security awareness training must be provided as part of new student induction processes with opportunities for regular refreshers made available thereafter.

3.2.3 Records demonstrating the completion of staff security awareness training should be maintained by the staff member and their line manager or at an appropriate departmental or organisational level.

3.3 **Job specific training requirements**

3.3.1 Some staff may have job functions which require additional information security training.

3.3.2 Royal Holloway will provide the additional training requirements as needed. (Examples may include staff who have access to systems that store confidential information or job responsibilities such as developers and database administrators.)

3.4 **Acceptable Use**

It is unacceptable for any person to use Royal Holloway, information technology resources:

3.4.1 In the furtherance of any illegal act, including violation of any criminal or civil laws.

3.4.2 In the furtherance of any act in violation of College Regulations, Policies and Standards.

3.4.3 To send threatening or harassing messages, whether sexual or otherwise.

3.4.4 To create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material capable of being resolved into obscene or indecent images or material unless lawful and properly supervised in for example, approved teaching or research.

3.4.5 To infringe any intellectual property rights (i.e. copyright infringement such as downloading music, video or other media-related files for non-business or academic purposes or storage of such files on network drives).

3.4.6 For any commercial purpose (i.e. for personal gain) which has not been sanctioned by the College.

3.4.7 For any political purposes which embrace extremism, racism, religious intolerance, advocate or support threats to life, advocate or support acts of terrorism or which threaten the United Kingdom's safety or economic wellbeing.

3.4.8 For any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs.

3.4.9 To use another individual's account, or to attempt to capture or guess other users' passwords.

3.4.10 To attempt to intercept access, amend, damage, delete or disseminate another person's files, emails, communications or data without the appropriate authority.

3.4.11 To distribute chain emails, or knowingly participate in fraud or be knowingly complicit, or behave in a negligent manner, in the distribution of malicious communications (i.e., phishing e-mails).

3.4.12 To libel or otherwise defame any person.

3.4.13 To provide unauthorised views or commitments that could appear to be on behalf of Royal Holloway.

3.4.14 To use any type of applications and/or devices to circumvent access management or security controls on Royal provided applications and service and/or devices.

3.4.15 To download or install unauthorised (e.g. unlicensed, pirated) software onto Royal Holloway managed or issued devices.

3.4.16 To attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

3.4.17 To use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) on the Royal Holloway information systems or network resources unless you have been specifically authorised to do so by the Chief Information Officer (i.e., delegated via the Cybersecurity team).

3.4.18 To use tools which would constitute a denial of service, or distributed denial of service attack.

3.5 **Email usage**

3.5.1 Do not conduct Royal Holloway's business or academic purpose, through a personal email account.

3.5.2 Do not use email accounts for commercial purposes unrelated to Royal Holloway's business or academic purpose.

3.5.3 Do not use a Royal Holloway email address for personal activities including purchasing and selling of goods, internet banking, or other sensitive personal correspondence (e.g., legal or medical).

3.5.4 You are advised not to use College email accounts for personal communication where possible, the incidental use of our systems to send personal email is permitted, subject to certain conditions. Personal use is a privilege and not a right

3.5.5 Personal uses must meet the following conditions:

3.5.5.1 It must be minimal and take place substantially outside of normal working hours (that is, during your lunch break and before or after work)

3.5.5.2 It must not affect your work or interfere with the business of the College

3.5.6 Do not send sensitive information to a personal e-mail account (i.e., sensitive information must not be sent outside of the Royal Holloway network via the sending, forwarding or redirection of e-mails to personal e-mail accounts.)
3.5.7 Do not send sensitive information to any recipient not authorised to receive such information.
3.5.8 Do not use email to transmit sensitive information in an unencrypted format.
3.5.9 Do not try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g., through misuse of scanned signatures)
3.5.10 Do not engage in mass transmission of unsolicited emails (SPAM).
3.5.11 Be vigilant to phishing emails and know how to spot and report suspicious emails.

3.6 **Secure workspace**
3.6.1 Staff are responsible for keeping all portable devices assigned to them safe and secure and must immediately report any loss or damage of their equipment to their line manager and the IT Service Desk.
3.6.2 Staff when travelling must carry laptops as hand luggage and avoid leaving portable devices vulnerable to theft (i.e. in sight in a parked vehicle or unattended in a public place).
3.6.3 Staff must keep their assigned workspace secure (e.g., lock confidential information in drawers, use cable locks) if issued by Royal Holloway.
3.6.4 Staff must be mindful of using mobile devices (e.g., smartphones and tablets) with access to Royal Holloway information and they should be secured with a password that meets any published College standard.
3.6.5 Documents containing sensitive information that are sent to a shared printer must be retrieved immediately to reduce the risk of unauthorised access.
3.6.6 Staff must return all Royal Holloway equipment and information assets when leaving Royal Holloway. Line Managers of Royal Holloway Staff must complete all appropriate exit procedures with leavers.

3.7 **Privacy and monitoring**
3.7.1 The access to and use of Royal Holloway owned information systems and assets is subject to monitoring and review, all users should have no expectation of privacy with respect to the Royal Holloway's communications systems.
3.7.2 Royal Holloway's communications systems (e.g., emails, instant messages, Internet usage) may be monitored, logged, reviewed, recorded and/or investigated to support the safety and security of its users and compliance with this policy.
3.7.3 Records of activity on these systems may be used by Royal Holloway and/or turned over to law enforcement authorities and other authorised third parties.
3.7.4 All users must be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic.
3.7.5 The College, when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace retains the right to inspect any user's computer, any information contained in it, and any information sent or received by that computer.

3.8 **Information protection requirements**
3.8.1 The confidentiality and integrity of information must be protected at rest, in use and in transit. Staff must adhere to the following guidelines.
3.8.2 Information at rest
3.8.3 Store College data on access-restricted / controlled Shared Folders or Drives (e.g., Departmental Share, College provided SharePoint resources).
3.8.4 Encrypt or password-protect removable media that contains confidential information such as USB drives and mobile devices.
3.8.5 Dispose of confidential information only after confirming compliance with records retention policies, regulatory requirements, or legal obligations.
3.8.6 Information in use
3.8.7 For access to systems that host sensitive information Staff must request access using an approved access request process/tool and be positively authenticated (i.e., have an established College Account in Active Directory or another Royal Holloway authorised authentication source).
3.8.8 Use the minimum amount of sensitive data, such as Personally Identifiable information (PII), necessary to support business operations.
3.8.9 Information in transit

3.8.10 Use Royal Holloway issued or approved encryption solutions to protect the integrity of confidential information that will be transmitted outside of Royal Holloway.

3.8.11 Information classification requirements

3.8.12 All users must adhere to any College published information classification system and ensure that appropriate measures are taken to protect information commensurate with its value to the College.

3.9 **User Authentication**

3.9.1 Users of Royal Information Systems must have an active user ID to access information assets on College networks.

3.9.2 Information assets that access or store or process sensitive information should authenticate a user's identity and a token in their possession (e.g., password and MFA application) prior to granting access.

3.9.3 User Access requests

3.9.3.1 Users must request access to technology infrastructure and/or applications required for job responsibilities using College approved access request processes and tools.

3.9.4 Principle of Least privilege

3.9.4.1 Users must not be granted access to technology infrastructure and/or applications that are not required to perform his/her job responsibilities. Managers and course tutors are responsible for ensuring their direct reports or students have the appropriate access to systems.

3.9.4.2 Reviews of user's access to applications and/or technology infrastructure will be performed by Managers at least annually to ensure access is appropriate to perform his/her job responsibilities.

3.9.5 Segregation of duties

3.9.5.1 Users must not be granted access to information assets that would allow entitlements to perform job responsibilities that are not compatible with each other (e.g., having the ability to both request and approve a change).

3.9.6 Password Protection

3.9.6.1 Passwords provide a foundational security control to protect access to systems, technology infrastructure, applications and information. Consider passwords as Confidential information and adhere to any Published Royal Holloway password requirements.

3.10 **Network Access**

3.10.1 Royal Holloway wired network access is restricted to authorized users only. Users must have a domain user identity to access the network.

3.10.2 Wireless Access

3.10.2.1 Wireless networks are inherently less secure than wired networks. Without using any application to support security and privacy, wireless networks should be regarded as being open and not secure.

3.10.2.2 At Royal Holloway University we have chosen not to encrypt our wireless traffic and use application encryption instead (such as HTTPS or SSH).

3.10.2.3 All users must assess the risks of using the Royal Holloway WI-FI network with sensitive information assets. Additional protection may be required when handling sensitive or confidential information using the Wi-Fi network.

3.10.3 Remote Access

3.10.3.1 Users who access the Royal Holloway network remotely must be authenticated prior to establishing a network connection.

3.11 **Physical Access**

3.11.1 Royal Holloway facilities that house systems, data and information assets must have appropriate physical access controls to protect them from unauthorised access.

3.11.2 Users must have a Royal Holloway identification and be prepared to show it, if requested by building security, IT Service Desk staff or the Cybersecurity team.

3.11.3 Only authorised persons are allowed into access-controlled areas. Visitors may be permitted access when authorised but must be escorted in controlled areas.

3.11.4 Circumventing established access control systems (e.g., propping doors open or tampering with turnstiles) is prohibited.

4. Roles and Responsibilities

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

4.2 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.

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

5. Related Documents

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

6. Monitoring and Compliance

6.1 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.

6.2 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.

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

7. Document Control Information

Policy Owner *(usually Director-level)*	Chief Information Officer
Approving Body	Executive Board
Approved on	16/02/2021
To be reviewed before	16/02/2022

Version History		
Version (newest to oldest)	Date of approval	Summary of changes
1.0	16/02/2021	First Approval