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 under the terms of the Royal Holloway: Acceptable Use of IT Policy.

1.2 Once a member of staff leaves the College or a student’s enrolment has ended such facilities are automatically withdrawn.

1.3 Certain staff members may retain some contact or role in the College beyond the term of their contract, for example as an Emeritus Professor, which may require them to retain agreed and well-defined access to College information assets.

1.4 Staff with College-owned IT Equipment are required to return it unless an exception is granted in line with this Standard.

1.5 Inactive IT accounts cause unnecessary expenditure on licensing and represent a significant cyber security risk to the College.

1.6 Former staff accounts and any accounts issued to external individuals requiring IT Access will be subject to closure and deletion following a period of inactivity defined within this Standard.

1.7 Access to student accounts is governed by student’s enrolment status and will be withdrawn in accordance with the timelines in this Standard.

2. Scope

2.1 This Standard applies to all users of Royal Holloway's computing resources, networks, data and information assets. Individuals covered by the Standard include Royal Holloway, staff, students, agents of the administration (e.g., contractors), external individuals (e.g., ‘visiting fellows’) and organisations who hold accounts accessing network services via Royal Holloway’s computing facilities and networks.

2.2 Royal Holloway Alumni Email for Life accounts are not in the scope of this standard.

2.3 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. Standard Statement

3.1 Responsibilities of Staff Leavers

3.1.1 Ensure their home address and personal contact details are up to date in the HR System.

3.1.2 Liaise with their line manager and colleagues regarding any relevant information assets on College provided personal storage, to ensure it is moved to a suitable location or deleted. Any encryption keys and or passwords associated with encrypted storage media should be securely communicated to the responsible information asset owner and or the line manager.

3.1.3 Liaise with their line manager and colleagues regarding any third-party account login details or service account credentials to ensure they are migrated to an alternative user or users and / or deleted.

3.1.4 Remove any personal information from their College provided personal storage and email account.

3.1.5 Save onto personally owned devices any personal records or confirmation of earnings they may need to retain. Staff may not copy or transfer any Royal Holloway information assets to personal storage without prior approval from the information asset owner or their line manager.

3.1.6 If required, to redirect their email account to a College email address nominated by the line manager and/or Head of Department/School/Service. Under no circumstances should a College email address be redirected to an external account.

3.1.7 Set up an “out of office” message on their email stating that they have left the College, giving a date of leaving and providing alternative College contacts (e.g, appropriate email and / or contact numbers).
3.2 Return of Staff IT Equipment

3.2.1 Heads of Departments/Schools/Services are responsible for ensuring the return of IT Equipment belonging to the College and that staff leavers comply with this Standard. Head of Departments/Schools/Services may wish to nominate a named individual to coordinate the return of IT Equipment by staff leavers.

3.2.2 Failure to ensure the return of centrally funded IT Equipment may result in the central provision of IT Equipment being unavailable for replacement or new posts within a Department/School/Service.

3.2.3 Centrally funded IT equipment that is returned should be passed to IT Services for appropriate sanitisation and preparation for re-use or disposal.

3.2.4 Prior to or on their last day of service staff leavers must:

3.2.4.1 Return all College owned IT equipment, including laptops, home desktops, monitors, mobile phones, tablets, all associated cables and power supplies and removable storage devices such as external drives and memory cards.

3.2.4.2 Remove all software licensed by the College from personally owned devices and return license keys to the appropriate information asset owner and/or line manager.

3.2.4.3 Remove any information or data belonging to the College from personal devices.

3.2.4.4 Dissociate their accounts and secure logins from single user devices and factory reset them.

3.3 Removal of Staff Accounts

3.3.1 Access to staff accounts will be withdrawn on their last day of service. All data associated with the account including, but not limited to, email, calendar, contacts and College provided private file storage will be retained for 90 days then permanently deleted.

3.4 Staff Retaining Access to Services after Leaving

3.4.1 Staff members who receive the title of Emeritus or other award approved by the Academic Staffing and Titles Committee may retain their IT Access, the HR Department will notify the IT Service Desk requesting continued access detailing which systems and data they require access to following the end of their employment contract.

3.4.2 If the staff leaver requires ongoing access to fulfil a role within the College or is awaiting the outcome of a decision that will necessitate ongoing access (e.g. the conferment of a Title) requiring them to retain IT Access, a Temporary IT Access Request may be submitted to the IT Service Desk by their Head of Department/School/Service for a time limited basis for up to one year, this request should detail which systems and data they require access to following the end of their employment contract.

3.4.3 To support managers in planning extended IT access for staff on fixed term contracts the HR Department will send notifications of expiry to Line Managers, Principal Investigators or Head of Department/School six months prior to their end date (for contracts that are under one year length this notification will be sent in accordance with the appropriate notice period).

3.4.4 The sponsor of a Temporary IT Access Request will consult with the College's Data Protection Officer to consider whether a Data Protection Impact Assessment (DPIA) process will be required based on the nature of the ongoing access requested.

3.4.5 Temporary IT Access Requests will not renew automatically, and a new request will need to be submitted prior to the end of the one-year extension.

3.4.6 The sign-up process for all staff retaining access to services after leaving will include a binding commitment to the College's Acceptable Use of Information Technology Standard and all associated, referenced policies and standards.

3.5 Staff Retaining Access to IT Equipment after Leaving

3.5.1 Centrally funded and managed IT Equipment must be returned to ensure compliance with licensing and contractual requirements and to allow redistribution and re-use.

3.5.2 Staff members who wish to retain departmentally funded IT Equipment after their last day of service may do so at the request of their Head of Department/School/Service to the IT Service Desk, approval to retain departmentally funded equipment will be at the discretion of the relevant Head of Department/School/Service.

3.5.3 Staff retaining departmentally funded equipment will not retain access to College managed software licenses, authentication, operating systems, contracts (e.g. mobile / data) or any form of ongoing College managed IT support without prior agreement as in section 3.4.

3.6 Student Leavers
3.6.1 Access to student accounts will be withdraw 190 days following their final day of enrolment. Data will be retained for a further 30 days then deleted.

3.6.2 Student email will be transitioned to the email-for-life service and access retained.

3.7 **Inactive Accounts**

3.7.1 IT accounts are deemed to be “inactive” and applicable for removal when a user does not carry out at least one of the following activities during a 180 day period:

3.7.1.1 Logging into any College managed application or service (such as Microsoft 365, Teams, Moodle) utilising their @royalholloway.ac.uk or @live.royalholloway.ac.uk credentials.

3.7.1.2 Logging onto a College managed computer or device.

3.7.1.3 Logging onto the College email system whether online, via a mobile device, tablet or computer via a mail client (such as Microsoft Outlook).

3.7.1.4 Connecting to the College via the Virtual Private Network Service.

3.7.2 Student IT accounts that are deemed inactive will be reported to Student Administration but their suspension and deletion will remain linked to enrolment status.

3.7.3 Accounts associated with salaried staff that are deemed inactive will be reported to HR for verification but their suspension and deletion will remain linked to their last day of service. This should ensure that staff are not impacted by the suspension of their account when on:

3.7.3.1 Long term sick
3.7.3.2 Family leave (including maternity, paternity, adoption)
3.7.3.3 Sabbatical or secondment
3.7.3.4 Jury service or service as an armed forces reservist

3.7.4 HR and Legal & Compliance may authorise an extension to the suspension and / or deletion of an IT Account.

3.7.5 All other IT accounts that are deemed inactive will be suspended and their users will be notified, if their account or extension of the account was approved by a Head of Department/School/Service they will also be notified.

3.7.6 If the user or the user’s original sponsor do not respond and take action to keep the account active, it will be deleted after a further 90 days.

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 Standard and may enlist other departments to assist in the monitoring and maintenance of compliance with this Standard.

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

5. **Related Documents**

5.1 Acceptable Use of Information Technology Policy.

6. **Monitoring and Compliance**

6.1 If for any reason users are unable to comply with this Standard 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 Standard 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 Standard must be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

7. **Document Control Information**
<table>
<thead>
<tr>
<th>Standard Owner (<em>usually Director-level</em>)</th>
<th>Chief Information Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approving Body</td>
<td>Executive Board</td>
</tr>
<tr>
<td>Approved on</td>
<td>13/04/2021</td>
</tr>
<tr>
<td>To be reviewed before</td>
<td>April 2023</td>
</tr>
</tbody>
</table>

**Version History**

<table>
<thead>
<tr>
<th>Version (newest to oldest)</th>
<th>Date of approval</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>N/A</td>
<td>First Draft – Internal IT Consultation</td>
</tr>
<tr>
<td>1.0</td>
<td>N/A</td>
<td>First Draft – Submitted for Approval</td>
</tr>
<tr>
<td>1.1</td>
<td>13/04/2021</td>
<td>Incorporated Executive Board feedback; HR to notify IT following conferment of honorary title; inclusion of process of notifications from HR as to expiring Fixed Term Contracts to ensure IT Access Extension may be made in a timely fashion</td>
</tr>
</tbody>
</table>