POLICY ON IT ACCESS FOR LEAVERS v2

Version Control and History

Title	Description	Author	Approved by	Date Approved
Policy on IT Access For Leavers Version 1.4	Policy on IT Access for Leavers	-	-	11/9/2017 (date posted to web site)
Policy on IT Access For Leavers Version 2	Policy on IT Access for Leavers	User Accounts Management Group (Information Services Directorate)	Information Strategy Committee	4/10/2023

Policy on IT Access for Leavers

The University of Strathclyde provides a wide variety of IT services, to staff to fulfil their roles within the Institution, and to students for use in their study and learning. Once a person leaves the University such facilities are automatically withdrawn. Individual data associated with the account, such as email, OneDrive for Business, Strathcloud and H: drive, are deleted at the same time as the account is deleted. This is in line with arrangements in most organisations. This document outlines the steps staff members and students should take when they plan to leave the Institution, and what other arrangements can be put in place.

Responsibilities of Staff Leavers

The University of Strathclyde requires all staff leavers to assist the University with its business continuity by taking certain steps **in advance of their departure**. Leavers should:

- Check that their address and personal contact details on Pegasus are up to date as vital information such as their P45 will be posted to their home address;
- Liaise with their line management and colleagues with regard to any relevant information that they have stored on their individual storage (such as OneDrive for Business, Strathcloud and H drive), or their University email, to ensure that the information is moved to a suitable location. To allow for business continuity, where this does not happen the University has a policy [Procedure for Accessing Personalised Electronic Storage Resources](#);
- Remove any personal information from their individual storage and email;
- Print or save onto personally-owned devices any payslips and P60 documents that they could need in future for their personal records or confirmation of earnings for mortgage applications and tax returns etc;

- Set up an "Out of Office" message on their email stating they have left the University, giving a date of leaving and who the alternative University of Strathclyde contact is. This "Out of Office" message should not contain any further information;
- Where deemed necessary and appropriate, a leaver may redirect their University email to a University of Strathclyde email address nominated by the leaver's line manager/Head of Department or School/Director. However, redirects should be used with caution, as emails to an individual may inadvertently contain personal data : for this reason, an "Out of Office" is usually more appropriate, see previous point. In the event that a redirect is set up, this must be to the email address of another member of staff or a role account belonging to the University of Strathclyde. Under no circumstances can a leaver's University email be redirected to a non-University account and the University reserves the right to immediately stop without warning any such redirection put in place.

For legal reasons the staff member must:

- Return all University-owned IT equipment, including home desktops, monitors, mobile phones, laptops and tablets. In some circumstances the University may allow such equipment to be purchased by members of staff. Staff members should discuss this with their line management prior to leaving. Where such devices are purchased they should normally be reformatted or reset to factory settings;
- Remove all software licensed by the University from personally-owned devices including MS Office and Operating Systems;
- Return any information or data belonging to the University held on personal devices or on paper off campus;
- Remove any information or data belonging to the University from personal devices and
- Return any keys and access control cards to their department/directorate.

Responsibilities of line-managers and departments

The line-manager and departments of staff leavers have a shared responsibility with the leaver, to ensure that the steps above are carried out. The primary responsibility remains with the leaver, but line-managers and departments should work with the leaver to ensure compliance.

Removal of Staff Accounts

Access to staff accounts will be withdrawn on the day they leave. The individual data associated with the account (for example, email, OneDrive for Business, Strathcloud and H: drive) will be retained for a six month period and then deleted.

Data which was created in shared areas by the account (for example, role mailboxes, Teams, SharePoint, i: Drive and research data repositories) will not be automatically deleted: it is the responsibility of the sponsors and business-owners of such shared facilities, to maintain and/or delete data as appropriate.

Staff Retaining Access to Services after Leaving

Exceptionally, if the leaver will retain some role within the University after they leave, a Temporary IT Access Request can be submitted by their Department, School, or Directorate for a time limited basis of up to one year. If they are continuing to collaborate with colleagues on My Place there is also an option for Limited Access Accounts through the IT Helpdesk or local Departmental/School IT staff. If they only need access in order to continue collaborating on Teams or SharePoint, then no user account is needed : instead, the Strathclyde staff who have access to the Team or SharePoint site can re-share the data with the leaver's external email address. In any of these cases, the department must ensure that the former employee only has access to relevant data.

If a staff member leaves and returns they will, whenever possible, get the same email address and login details as they had previously.

Student Leavers

Student email and individual storage services can be withdrawn as soon as the individual ceases to be a student of the University. However, in normal circumstances, such services are retained until 3-6 months after the student has completed their studies. The 'student' status of the account switches automatically to 'affiliated' 1 month after completion preventing the account access to software downloads or external library resources to ensure the University remains compliant with supplier licence agreements. Completed students are warned before accounts are deactivated.

If a student leaves and then returns to undertake a different course or postgraduate research they will, whenever possible, retain the same email address and login details for up to one year after the completion of their previous course.