# Policy: Gaining access to data and resources in exceptional circumstances.

|  |  |  |
| --- | --- | --- |
|  |  | Version 1.3 |
|  | | Gaining access to data and resources in exceptional circumstances. |
|  | | **the place of useful learning**  The University of Strathclyde is a charitable body, registered in Scotland, number SC015263 |

|  |  |  |  |
| --- | --- | --- | --- |
| Version control and history | | | |
| Title | Description | Author | Approval Date |
| Gaining access to data when owner unavailable | First draft | Bruce Rodger | 11/7/2024, presented to ISOWG |
| V1.2 | More detail on applicability to shared data following feedback from ISOWG | BR/Andrew Edmond |  |
| V1.3 | Extension to cover (e.g.) Teams resources  Change of title | BR/AE/Elaine Grant | To be approved by ISSRG April 2025 |
|  |  |

# Background

Definitions:

* “Individual data services”: services for storing data which is normally accessible only to one person. For example, individual email, H: drive, OneDrive.
* “Shared data services”: services for storing data which is normally accessible to multiple people. For example, role-based email (e.g. admissions@strath.ac.uk), i: drive, Sharepoint and Teams.
* “Owner”: in the case of individual data services, the one user who normally has or controls access to the data; in the case of shared data services, the user or users who control who can access the data. While the term “owner” is commonly used in this context, “custodian” may be more correct; University data is owned by the University.

There is often a business need, including as part of the University Business Continuity arrangements, to access University data, when the account owner is unavailable or unable to authorise access, or it is necessary to do so without the account owner’s knowledge or permission. This may be for a variety of reasons, including: annual leave, illness or incapacity, legal/disciplinary/investigation action, official investigations by third parties, e.g. police etc.

The data required may be held within an individual data service, such as personal University email or filestore (H: drive, OneDrive) or a shared data service, e.g. shared mailbox, I Drive, Teams and Sharepoint sites. The principles described below apply irrespective of the technology or the type of service (individual or shared.

The general principles described below will also apply to “ownership” or administrative access to shared materials or online resources – e.g. if the owner of an active Teams or Sharepoint site has left the University, the processes described below would also allow assignment of a new site owner.

It should be noted that while individual data services such as email are provided to staff solely for use in relation to their work, there will undoubtedly be some personal, private and sensitive information held within them, including potentially emails from HR or trade unions. Thus, there may be legal, data protection and privacy implications for the University and its staff in providing such access. Similar issues may also exist in relation to shared data services. These issues should be considered fully when assessing the need to access resources.

Therefore, formal procedures are required to ensure that the University can continue its business.

The procedures and processes set out in this document should be followed unless the specific circumstances dictate that a bespoke arrangement is required and agreed between relevant areas. This is only relevant in the most complex and sensitive of matters and will not be considered for ‘routine’ requests.

This document supersedes the previous “Procedure for Accessing Personalised Electronic Storage Resources”.

# Avoiding the situation

Ideally, this situation would not arise – key data should not be held solely by one individual; nor should access to shared data be controlled solely by one individual. All areas of the University ensure that critical data can be accessed/controlled by multiple people as part of their Business Continuity procedures.

University departments should take action to minimise the occasions when they may require access to the contents of mailboxes and file stores (etc) allocated to individuals. Appropriate use should be made of role-based email and group storage instead of individual OneDrive and H: drive storage. Furthermore, where group storage is used, departments should ensure that more than one person can control access: for example, every Microsoft Team or Sharepoint site should have more than one owner.

Doing this may negate or reduce the need for an emergency access procedure at a later date.

When an employee is leaving the University or changing their role, their line manager should ensure that they make appropriate arrangements to handover relevant information in advance of their departure. When someone leaves the University they should be asked to remove any information personal to them. Guidelines, including a checklist of actions, for managers and staff on access for staff leavers and movers are available on the University’s People Hub.

**Under no circumstances should anyone share – or be asked to share - their password or login credentials with a colleague.**

# If access is required to an **individual** data service

## Where the account owner is temporarily unavailable

The line manager and/or Head of Department[[1]](#footnote-2) should determine whether it is appropriate in the circumstances to contact the account owner. This will depend on the specific circumstances and may require input from colleagues in other areas, e.g. HR. If it is deemed to be appropriate to contact the account owner, there are two options available.

## Option 1 – Contact the account owner and ask them to forward the data

The line manager or Head of Department should contact the account owner, explain the situation, and ask for their assistance. If in agreement, the account owner should be asked to forward the data on, or to enable sharing. If this option is available, it is often the simplest process.

If they do not agree see Option 3.

## Option 2 – Contact the account owner and gain authorisation for a colleague to access the account

The line manager or the Head of Department should contact the owner to explain the situation and ask for their assistance.

If in agreement, the account owner should be requested to provide written authority for an appropriate individual, as approved by the University, to access the information within the account.

**Under no circumstances should the account holder be asked for or disclose their login credentials.**

The written authority should be passed to Information Services (via the Help Desk) who will arrange supervised access to the resource. If appropriate and possible, the account owner would be allowed to be present while the resource was accessed or to arrange to remove personal information prior to the access.

If they do not agree, see Option 3.

## Option 3 – The member of staff is unavailable, unwilling to agree, or it is otherwise inappropriate to contact them

If the account holder is unavailable, or unwilling to grant access, or requesting their assistance is deemed to be inappropriate, a formal request should be made for access. The request should be made to the Information Services helpdesk, who will forward it to one of the Information Services Assistant Directors for further action.

The request must include:

* Details of the resource (i.e. email address, H drive, SharePoint, Teams etc)
* For emails: details to enable relevant material to be identified, e.g. time period, subject matter, sender/recipients etc.t
* An explanation of the circumstances which have necessitated this request

In some cases, it may be necessary to have the request approved/reviewed by Human Resources, the Information Governance Unit, Legal Services, or other parts of the University. Once verified, Information Services will facilitate supervised access to the appropriate data for a limited time period.

Where access to the account is authorised, all actions must be fully documented and, while information may be copied, no information should be deleted or amended other than in exceptional circumstances for legal, compliance or other significant reasons and only following consultation with relevant senior colleagues.

When accessing an email account, no messages may be sent externally from the account, however obviously business-related emails can be forwarded to an account determined by the Head of Department. Any obviously personal information must not be accessed unless relevant to an investigation. On confirmation to the Help Desk of the completion of the appropriate actions access to the accounts will be removed.

# If access is required to a **shared** data service

## If the shared data service account owner is temporarily unavailable

For shared data, a common scenario is that there is nobody available who can control access to the data. Therefore, although there are people available who can access the data, they cannot enable (or disable) access for other people. For example, this situation arises when a Microsoft Team has one owner and many members: the members are available, but the team owner has left the University. If someone else then needs to be added to the team, the members are unable to add them.

## Option 1 – Workaround the problem until the shared data service owner is available

Consider whether access to the data can be provided by some other means, on a temporary basis. For example, users with access to the data could provide a copy of it to the user(s) who need it, through a different technology, e.g. email, until the data owner is available again.

## Option 2 – Contact the shared data service owner and ask them to enable access

If possible and appropriate, the line manager or Head of Department of the shared data service owner should contact the shared data service owner to explain the situation and ask for their assistance.

The shared data service owner should be asked to enable access for the users who require it.

## Option 3 – Contact the shared data service owner and gain authorisation for access to be given

If possible and appropriate, the Head of Department of the shared data service owner should contact the shared data owner to explain the situation and ask for their assistance. If in agreement, the data owner should be requested to provide written authority for access to be given to the individual(s) who require it.

**Under no circumstances should the data owner be asked for or disclose their login credentials.**

The written authority should be passed to Information Services (via the Help Desk) who will arrange for the administrators of the relevant system to grant access.

## Shared data service owner is unavailable, unwilling to agree to access, or it is inappropriate to contact them

If the data shared data owner (or owners, if there is more than one) is unavailable or unwilling to grant access, or requesting their assistance is deemed to be inappropriate, a formal request should be made for access. The request should be made to the Information Services Helpdesk, who will forward it to one of the Information Services Assistant Directors for further action. The request would normally be submitted by, or verified by, the line manager of the data owner who is unavailable.

The request must include:

* Details of the resource (i.e. SharePoint site name, Team name etc)
* An explanation of the circumstances which have necessitated this request

In some cases, it may be necessary to have the request for access approved/reviewed by Human Resources, the Information Governance Unit, Legal Services, or other parts of the University. Once verified, Information Services will facilitate a suitable level and duration of access to the appropriate data.

# Procedures

The technical procedure to gain authorisation and to enable access to a mailbox, to filestore and to similar resources is defined in a Helpdesk Standard Operating Procedure.

1. In this document, the term 'Head of Department' should also be taken to include staff with equivalent seniority in the University hierarchy, even if they are not officially a ‘Head of Department’ e.g. Professional Services Directors, Deans and Senior Officers or Faculty Managers. [↑](#footnote-ref-2)