Document Control
This document is subject to change control and any amendments will be recorded below.

Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Location</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1-0</td>
<td>06/10/16</td>
<td>Security-Team share</td>
<td>1st draft</td>
</tr>
<tr>
<td>0-2-0</td>
<td>10/10/16</td>
<td>Security-Team share</td>
<td>Annexes added</td>
</tr>
<tr>
<td>1-0-0</td>
<td>10/11/16</td>
<td>IT Intranet</td>
<td>0-2-0 approved by ITSG and becomes 1-0-0</td>
</tr>
</tbody>
</table>

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at http://it.leeds.ac.uk/info/116/policies. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.
Contents

1. Introduction ......................................................................................................................................................... 4
1.1. Background ................................................................................................................................................. 4

2. Use of User Accounts ........................................................................................................................................ 4
2.1. Passwords ................................................................................................................................................... 4

3. Controlling Shared and Other Accounts .......................................................................................................... 4
3.1. Shared Access and Project Accounts ......................................................................................................... 4
3.2. Temporary Accounts ................................................................................................................................... 4
3.3. Conference and Visitors’ Accounts ............................................................................................................. 5
3.4. Lecture Theatre Computers ........................................................................................................................ 5

4. Third Party Access to Email and File Stores ................................................................................................... 5
4.1. Allowing Others to Access Your Email ........................................................................................................ 5
4.2. Continued Access to Email after University Employment ........................................................................... 5
4.3. Sharing Your Data ....................................................................................................................................... 5
4.4. Third Party Access to Accounts – Expected Absence ................................................................................. 6
4.5. Out of Office Notification ............................................................................................................................. 6
4.6. Third Party Access to Accounts – Unexpected Absence .............................................................................. 6
4.7. Access to Accounts of Former Employees - DS and Admin Domains ........................................................ 6
4.8. Control and Accountability of Student Accounts ......................................................................................... 6
4.9. Confirmation of Student Receipt of Email ................................................................................................... 6
4.10. Temporary Disablement Account ................................................................................................................ 7

5. Dealing with Misuse, Abuse and Illegal Activity .............................................................................................. 7
5.1. Allegations ................................................................................................................................................... 7

6. Annexes ............................................................................................................................................................... 8
6.1. Annex A - Preparing for Staff Leaving ......................................................................................................... 8
6.3. Annex C – 3rd Party Access to Staff Emails and File Store ........................................................................ 10
6.4. Annex D – Accessing Emails or Data of Former Employees ...................................................................... 11
6.5. Annex E – Checking whether a Student has received an Email .................................................................... 12
6.6. Annex F – Temporary Disablement of User Accounts .............................................................................. 13
6.7. Annex G - Dealing with Police Requests for Data ....................................................................................... 14
1. **Introduction**

1.1. **Background**

This Standard delivers the requirements for members of the University to fulfil the requirements of University’s Access Control and Account Management Policy\[1\].

2. **Use of User Accounts**

2.1. **Passwords**

In accordance with the Password Usage and Management Policy all users are required to change their initial log-on password the first time that they log onto a system where the system itself does not automatically enforce this requirement.

3. **Controlling Shared and Other Accounts**

3.1. **Shared Access and Project Accounts**

When there is a requirement for several users to access common data and mailboxes, for example when working collaboratively, shared areas are to be created and these are to be accessed through the use of each user’s own user account.

In some cases, a project account may be permitted whereby members of a ‘group’ access the account through the use of a common (shared) user-name and password. In such cases access must be tightly controlled by the ‘account holder’ as the degree of accountability associated with personal accounts is diminished when using project accounts.

On all such occasions the account holder is responsible for maintaining a list of all users who have been granted access to the account at any given time, and for ensuring that the password is changed whenever a user leaves the project team.

3.2. **Temporary Accounts**

Faculties, schools and departments that have a high turn over of temporary or agency staff may utilise temporary accounts. In all such cases a named custodian (and deputy) will be responsible for managing them.

Each temporary account is to be set with a master password which is only known by the custodian and his/her deputy and this must be changed to a previously unused user-password each time an account is issued.

Temporary accounts must not to be issued until each new user signs a form to confirm that they will abide by the Use of Computer Systems Policy. Once signed, forms are to be retained locally for a period of 12 months after the user has left, and presented to auditors or member of the IT Security Team on request.

The custodians of temporary accounts are responsible for managing the master password, in accordance with the Password Usage and Management Policy, as soon as a temporary user no longer requires access to the respective system.
3.3. Conference and Visitors’ Accounts

Faculties, schools and departments that are allocated a block of user-accounts (user-names and passwords) by IT User Administration are to appoint a custodian and a deputy to manage them.

Prior to issuing an account the custodian / deputy is responsible for ensuring that each user signs a form to confirm that they will abide by the Use of Computer Systems Policy. Once signed, forms are to be retained locally for a period of 12 months after the user has left, and presented to auditors or member of the IT Security Team on request.

Individuals who are given a conference or visitors’ account are to be instructed to immediately change their password. Instructions on how to do this are available at http://it.leeds.ac.uk/info/77/managing_your_account/10/how_to_reset_your_password.

User-account custodians are to notify IT Username Administration of lapse dates as they issue these accounts, or for emailing a lapse request to sysadmin@leeds.ac.uk when the users no longer require access to University systems.

3.4. Lecture Theatre Computers

Visitors to lecture theatres are to be issued with temporary accounts as described at 3.2 above. These are to be managed by Conference Office staff in accordance with the requirements of this Standard.

4. Third Party Access to Email and File Stores

4.1. Allowing Others to Access Your Email

Members of staff using Outlook are to assign delegated rights to their mailbox if they have a need for someone else to access their email, for example, secretaries on a permanent basis, or staff covering a particular role during periods of temporary absence. Instructions on how to do this are available here.

4.2. Continued Access to Email after University Employment

Where there is a requirement for the University to maintain access to an email account for business continuity reasons after the account holder has left University employment, staff are to make arrangements for this prior to their final day. Where such arrangements are not put in place, IT will take action to implement it. Please see process TPA-1-2 at Annex A for further details.

4.3. Sharing Your Data

Where there is a requirement to share access to data, the public folders on the N: Drive are to be used with permissions restricted, as appropriate, to the individuals who need to share it.

If there is a need for shared access to classified data please contact the IT Service Desk to enquire about the use of encryption software.
4.4. **Third Party Access to Accounts – Expected Absence**

Prior to staff leaving work for known absences (leave, maternity leave, planned surgery etc.) they are to provide another member of staff with delegate access to their mailbox, in accordance with 4.1, if ongoing access to their email account is required for operational purposes during their absence.

4.5. **Out of Office Notification**

When staff are going to be absent from work they are responsible for setting their own out of office automated reply on their email account. Where staff are unexpectedly absent from work and are unable set their own out of office automated reply the school or department in which they work can request IT to set it for them in accordance with process TPA-1-1 which can be found at Annex B.

4.6. **Third Party Access to Accounts – Unexpected Absence**

Where school/departmental access is required to a member of staff’s email account or personal file store during a period of unexpected absence, applications are to be submitted to the IT Service Desk using the form that can be found here. IT will manage the application in accordance with TPA-1-4 which can be found at Annex C.

Subject to the requirements of each application, a third party will be given access to the absentee’s mailbox, file store or both mailbox and file store. Once this has been done, an email will be sent by IT to the account holder and the third party (copied to cybersecurity@leeds.ac.uk) confirming the action.

4.7. **Access to Accounts of Former Employees - DS and Admin Domains**

Heads of Schools or services requiring emails or data of former employees are to stipulate the email subject or data that they require and IT will make a copy available to them or their nominee.

In circumstances where the full details of the required data are not known, the applicant or their representative will be provided with supervised access to the respective account within IT and IT staff will transfer a copy of the data to the required account once verified that it is work-related.

IT will manage the application in accordance with TPA-1-5 which can be found at Annex D.

4.8. **Control and Accountability of Student Accounts**

It is the responsibility of computer support staff in faculties and schools to ensure that their students are aware that their accounts may be accessed for both teaching and computer account management purposes. Ideally this notification should be given in writing at the start of each academic year.

4.9. **Confirmation of Student Receipt of Email**

When a school or department requires conformation as to whether a student has received an email and whether this is shown in their mailbox as having been read, they are to follow process TPA-1-5 which can be found at Annex E.
4.10. Temporary Disablement Account

IT will manage the temporary disablement of user accounts in accordance with the process which can be found at Annex F.

5. Dealing with Misuse, Abuse and Illegal Activity

5.1. Allegations

All allegations of account misuse, abuse or illegal activity will be investigated in accordance with the Security Incident and Computer Misuse Policy.

IT will manage the application in accordance with the process which can be found at Annex G.
6. Annexes

6.1. Annex A - Preparing for Staff Leaving

START HERE
Member of staff is about to leave the University and the school/department needs to make arrangements for continuity when they have left.

Agree with the member of staff an out of office message for their account when they leave.

Staff member enables the out office on or close to their last day or sets it on a timer. If member of staff uncooperative follow process at TPA-1-1

Agree with the staff member the work data you need access to.

Do they have work related data on their M: drive?

Yes

Staff member moves the data to a secure location (or N: Drive as appropriate) where delegated individuals can access it.

No

Do you need access to emails they receive?

Yes

Will they permit you email delegate access?

Yes

Staff member enables delegate access

No

Will they assign rules to forward emails you need?

Yes

Staff member assigns rule to forward emails required

No

Send an email to itservicedesk@leeds.ac.uk with the subject "TPA-1-2-user leaving" and provide details of the staff username, leaving date and time period for out of office (typically 1 to 3 months).

IT Service Desk creates Catalogue Task and assigns to IT Username Admin.

IT Username Admin. decline request and inform requester

Request Valid?

Yes

IT User Admin change user password on leaving date and leave account active for requested time.

Requester informed and told to follow process at TPA-1-3 if access to the account is required.

Task closed
6.2. Annex B – Setting an Out of Office Notification

**Process for setting an Out of Office for staff who are unable to set their own**

- **START HERE**
  - Member of staff is absent from work and not in a position to set their out of office notification

- Send an email to itservicedesk@leeds.ac.uk with the subject "TPA-1-1-out of office" and provide out of office text

- IT Service Desk creates Catalogue Task and assigns to IT Username Admin.

- IT Username Admin validate the person requesting the out of office and the suitability of the text

- **Request valid?**
  - **YES**
    - IT User Admin assigns to Windows Server Team
    - Out of office message applied
    - Inform requestor
  - **NO**
    - IT Username Admin decline request and inform requester

- **Task closed**
6.3. Annex C – 3rd Party Access to Staff Emails and File Store

Follow flowchart TPA-1-3

Has the member of staff left University employment?

YES

Complete a Third Party Access Request Form and submit via an email to the IT Service Desk itservicedesk@leeds.ac.uk with the subject "TPA-1-4-access to user account required"

NO

Follow flowchart TPA-1-3

Request Valid?

YES

IT Username Admin validate the person requesting access as having the authority to do so – i.e. school/ department and position

NO

IT Username Admin decline request and inform requester

IT Username Admin assigns to Windows Server Team

Supervised third party granted access to account for period required

Access revoked

END

IT Service Desk prints form and obtains signature from member of IT exec authorising the request

IT Service Desk creates Catalogue Task and assigns to IT Username Admin. Fully signed form attached to Catalogue Task

IT User Admin assigns to Windows Server Team

Supervised third party granted access to account for period required

Access revoked

Task closed

IT User Admin validates request and informs requester

Task closed

IT Service Desk prints form and obtains signature from member of IT exec authorising the request

IT Service Desk creates Catalogue Task and assigns to IT Username Admin. Fully signed form attached to Catalogue Task

IT User Admin assigns to Windows Server Team

Supervised third party granted access to account for period required

Access revoked

Task closed
6.4. Annex D – Accessing Emails or Data of Former Employees

**START HERE**
Access required to former member of staff’s email or file store

Send an email to `itservicedesk@leeds.ac.uk`
With the subject "TPA-1-3-access to user account required" stating:
(1) the name of the user(s),
(2) the names or content, file(s) or email(s) that you need, or
(3) if you need supervised access

Is the individual still left employment and is not re-employed elsewhere within University?

**NO**
IT Username Admin. decline request, close Catalogue Task and inform requester

**YES**
IT Service Desk creates Catalogue Task and assigns to IT Username Admin. To check

Is the requestor from the correct school/Department and do they have the correct authority?

**NO**
IT Username Admin. decline request, close Catalogue Task and inform requester

**YES**
IT User Admin assigns to Windows Server Team

Windows Server Team searches for emails or files requested

Are the names of the files(s) or email(s) known?

**NO**
Windows Server Team search emails or files requested

**YES**
Windows Server Team contact you and arranges an appointment with you

Is the data found?

**NO**
Requestor informed

**YES**
Windows Server Team copy email or data to your account

Requestor informed

Is the requestor from the correct school / Department and do they have the correct authority?

**NO**
Has individual left employment and is not re-employed elsewhere within University?

**YES**
NO

Windows Server Team copy email or data to your account

Requestor informed

Windows Server Team copy email or data to your account

Requestor informed

Task closed

Requestor informed

Task closed

Task closed

Or restart process requesting supervised access

Task closed
6.5. Annex E – Checking whether a Student has received an Email

START HERE
A member of staff needs to know if a student has read an email

Send an email to itservicedesk@leeds.ac.uk with the subject “TPA-1-5-student read receipt required” and provide details of the student and email

IT Service Desk creates Catalogue Task and assigns to IT Username Admin.

IT Username Admin validate the person making the request – i.e. correct school

Request valid?

YES
IT User Admin assigns to Windows Server Team
Windows Server Team check student mailbox.
Inform requestor

NO
IT Username Admin decline request and inform requester

Task closed

Task closed
6.6. Annex F – Temporary Disablement of User Accounts

**IT Security: 2016**
**Temporary Disablement of User Accounts**

---

**Requirement for a staff user-account to be temporarily disabled**

Username Administration contacted and requested to disable user account

- **NO**
  - Requestor informed that they have to route the request via the correct authority
  - **Task end**

- **YES**
  - Has the request come from the correct authority?*
    - **NO**
      - Is the request by telephone or email?
        - **Telephone**
          - IT Username Administration action the request but ask requestor to send email confirmation for audit trail purposes
          - **Account disabled and ServiceNow Service Request closed**
          - Username Administration contacted and requested to reinstate the user account
          - **Has the request come from the correct authority?**
            - **NO**
              - **Task end**
            - **YES**
              - **Telephone**
                - IT Username Administration action the request but ask requestor to send email confirmation for audit trail purposes
              - **Email**
                - IT Username Administration create a Service Request in ServiceNow assigned to their own group and record number in IDM database
                - Account disabled and ServiceNow Service Request closed
              - Username Administration contacted and requested to reinstate the user account
              - **Has the request come from the correct authority?**
                - **NO**
                  - **Task end**
                - **YES**
                  - **Telephone**
                    - IT Username Administration action the request but ask requestor to send email confirmation for audit trail purposes
                  - **Email**
                    - IT Username Administration create a Service Request in ServiceNow assigned to their own group and x-ref to previous Service Request which asked for account to be disabled
                    - Account reinstated & task closed

**Requirement for a student user-account to be temporarily disabled**

- **YES**
  - Has the request come from the correct authority?*
    - **NO**
      - Is the request by telephone or email?
        - **Telephone**
          - IT Username Administration action the request but ask requestor to send email confirmation for audit trail purposes
        - **Email**
          - IT Username Administration create a Service Request in ServiceNow assigned to their own group and record number in IDM database
          - Account disabled and ServiceNow Service Request closed
          - Username Administration contacted and requested to reinstate the user account
          - **Has the request come from the correct authority?**
            - **NO**
              - **Task end**
            - **YES**
              - **Telephone**
                - IT Username Administration action the request but ask requestor to send email confirmation for audit trail purposes
              - **Email**
                - IT Username Administration create a Service Request in ServiceNow assigned to their own group and x-ref to previous Service Request which asked for account to be disabled
                - Account reinstated & task closed

* The Secretary to the University
  The Deputy Secretary
  Director or Deputy Director HR
  University’s Legal Advisor
  Director IT
  Members of the IT Security Team
6.7. Annex G - Dealing with Police Requests for Data

START HERE

Police contact IT and request staff or student data relating to an incident or investigation

Direct officer to IT Security Team office and call IT Security Team to notify

Enquire police officer is on campus?

NO

POLICE CONTACT IT AND REQUEST STAFF OR STUDENT DATA RELATING TO AN INCIDENT OR INVESTIGATION

IT Security Team log details in Security Team Incidents with ServiceNow - Incident number

Police officer instructed to submit form DP7 (Section 29 (3) Data Protection Act) to Secretariat

Police officer submits form DP7 (Section 29 (3) Data Protection Act) to Secretariat

Secretariat approve the request?

NO

NO

NO

NO

Incident closed

YES

Is the police officer on campus?

IT Security Team take the call and create an incident in ServiceNow assigned to IT Security Team - ServiceNow log must not contain any details of case which identify data subjects

Establish if the requirement for data urgent?

YES

IT Security Team instructed by Secretariat to serve the request

IT Security Team speak with respective team, obtain required data and update ServiceNow Incident

Information given to police officer or to Secretariat for handover as instructed

ServiceNow Incident closed and IT Security Team log relating to incident updated

Secretariat approve the request?

YES

Police officer instructed to submit form DP7 (Section 29 (3) Data Protection Act) to Secretariat

Inform police officer that a form DP7 is required (Section 29 (3) Data Protection Act) and to contact Roger Gair, David Wardle or Adrian Slater (Secretariat) once available

YES

Is DP7 is required (Section 29 (3) Data Protection Act)

Police officer instructed to submit form DP7 (Section 29 (3) Data Protection Act) to Secretariat

Information given to police officer or to Secretariat for handover as instructed

YES

Direct officer to IT Security Team office and call IT Security Team to notify

Refer police officer to Roger Gair, David Wardle or Adrian Slater (secretariat)

Establish if the requirement for data urgent?

NO

IT Security Team instructed by Secretariat to serve the request

IT Security Team speak with respective team, obtain required data and update ServiceNow Incident

Information given to police officer or to Secretariat for handover as instructed

ServiceNow Incident closed and IT Security Team log relating to incident updated

Secretariat approve the request?

NO