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>Circulation</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>04/07/05</td>
<td>Old IT website</td>
<td>First Formal Issue</td>
</tr>
<tr>
<td>1.1</td>
<td>08/07/05</td>
<td>Old IT website</td>
<td>Change to Appendix to reflect segregation of forms</td>
</tr>
<tr>
<td>1.2</td>
<td>13/08/05</td>
<td>Old IT website</td>
<td>Addition of text to 4.3</td>
</tr>
<tr>
<td>1.3</td>
<td>25/10/05</td>
<td>Old IT website</td>
<td>Removal of ‘common information’ in Section 1 and Section 2.7 largely replaced by Password Usage and Management Policy</td>
</tr>
<tr>
<td>1.4</td>
<td>24/03/06</td>
<td>Old IT website</td>
<td>Section 5 and Removal of Appendices</td>
</tr>
<tr>
<td>1.5</td>
<td>21/06/06</td>
<td>Old IT website</td>
<td>Replacement of Section 5 to 5.3 inclusive.</td>
</tr>
<tr>
<td>1.6</td>
<td>09/08/07</td>
<td>Old IT website</td>
<td>Replacement 3.2; new 5.1 and 5.2; most of 5.4 deleted; Appendix deleted; general review</td>
</tr>
<tr>
<td>1.7</td>
<td>04/08/09</td>
<td>Old IT website</td>
<td>New 5.6 governing 3rd party access to data and emails of those leaving under PRT/MIS</td>
</tr>
<tr>
<td>1.8</td>
<td>09/05/15</td>
<td>IT Security Website</td>
<td>Update to Sections 3.2 and 5.8</td>
</tr>
<tr>
<td>1-8-1</td>
<td>08/09/16</td>
<td></td>
<td>Split into Policy and Standard</td>
</tr>
<tr>
<td>1-8-2</td>
<td>12/10/16</td>
<td></td>
<td>Correction of typos and addition of URLs</td>
</tr>
<tr>
<td>1-8-3</td>
<td>2/11/16</td>
<td></td>
<td>Feedback from Will Crocombe &amp; Dave Neild</td>
</tr>
<tr>
<td>2-0-0</td>
<td>10/11/2016</td>
<td>IT Security Website</td>
<td>Approved by ITSG. Version 1-8-3 becomes 2-0-0</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/250/access_control_and_account_management_policy. 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. **Creating, Controlling and Managing User Accounts** ................................................. 4  
   2.1. Account Creation ......................................................................................................... 4  
   2.2. Conditions of Acceptance .......................................................................................... 4  
   2.3. Identification, Authentication and Traceability ......................................................... 4  
   2.4. Password Change at Initial Log-on .............................................................................. 5  
   2.5. Account Privileges ..................................................................................................... 5  
   2.6. Staff Account Management ......................................................................................... 5  
   2.7. Student Account Management ..................................................................................... 6  

3. **Use of Accounts** .......................................................................................................... 6  
   3.1. Account Restrictions ................................................................................................... 6  
   3.2. Access Parameters ..................................................................................................... 6  

4. **Controlling Shared and Other Accounts** .................................................................. 6  
   4.1. Shared Access and Project Accounts ........................................................................... 6  
   4.2. Conference and Visitors’ Accounts ............................................................................. 7  

5. **Third Party Access to Email and File Stores** ............................................................... 7  
   5.1. Allowing Others to Access Your Email ....................................................................... 7  
   5.2. Sharing Your Data ...................................................................................................... 7  
   5.3. Third Party Cover Arrangements for Known Absence of Staff ................................ 7  
   5.4. Management Third Party Access to Email and Data .................................................. 7  
   5.5. Third Party Access during Unexpected Staff Absence ............................................. 7  
   5.6. Approval and Authority - Third Party Access during Unexpected Staff Absence .......... 8  
   5.7. Access to Accounts of Former Employees - DS and Admin Domains ..................... 8  
   5.8. Third Party Restrictions ............................................................................................. 8  
   5.9. Control and Accountability of Student Accounts ....................................................... 8  

6. **Dealing with Misuse, Abuse and Illegal Activity** ......................................................... 9  
   6.1. Requests for Account Access by the Police and Law Enforcement Agencies ............. 9
1. Introduction

1.1. Background

The ever increasing use of digitised and networked information at the University intensifies the risk of data being copied or stolen, or modified, hidden, encrypted or destroyed. Unless access to our systems is appropriately managed, there is an increased risk that unauthorised persons will obtain use of our resources and gain access to University data.

Although technical controls provide an essential element of overall protection, they only deliver a percentage of the required solution, the most effective defence being achieved through awareness and good working practices.

This document forms the University’s Access Control and Account Management Policy in support of the [http://it.leeds.ac.uk/info/116/policies/249/information_protection_policy](http://it.leeds.ac.uk/info/116/policies/249/information_protection_policy). It concerns the use and management of logon credentials for University computer accounts (user-ids and passwords), extending to the management of third party access to accounts and data. Compliance with this Policy will enable consistent controls to be applied throughout the University minimising exposure to security breach, whilst allowing systems administration and technical support staff to conduct their activities within the framework of the law.

Mechanisms required to achieve compliance with this Policy are defined in the Access Control and Account Management Standard [i1].

2. Creating, Controlling and Managing User Accounts

2.1. Account Creation

User-accounts [WC2] will only to be created on the correct authority. It is the responsibility of the system administrator who is creating user-accounts to confirm that the correct level of authority has been granted.

2.2. Conditions of Acceptance

Prior to the creation of a computer account users are required to record their agreement to comply with the Use of Computer Systems Policy and other relevant policies. These agreements will be retained throughout the lifetime of the accounts and for a period of twelve months after accounts have been lapsed.

2.3. Identification, Authentication and Traceability

All users of University systems must be identified and authenticated as a valid user prior to access being granted to computer resources, allowing activities performed traceable to individual account holders [WC4][3].

Mechanisms such as tokens, biometric readers or digital certificates may be used in addition to passwords for the identification and authentication of users.
2.4. **Password Change at Initial Log-on**

Where possible, systems are to be configured to force users to change their password at their first logon.

2.5. **Account Privileges**

Account profiles and privileges are to be restricted to the minimum required for individual account holders to fulfil their role.

Access to operating systems and applications is to be generally restricted to designated administrators and support staff associated with the management and maintenance of the respective platforms.

User privileges are to be reviewed on a regular and frequent basis and withdrawn where the circumstances of those who have been granted privileges no longer warrant such access.

2.6. **Staff Account Management**

2.6.1 **Currency**

User-accounts are only to remain active for the period required for individual users to fulfil the needs for which they were granted.

2.6.2 **Management of Local Systems Accounts**

Faculty, School and departmental staff who administer their own local systems are to arrange with Human Resources to receive notification when members of staff either leave University employment, or transfer to a job outside their domain.

Administrators are to implement a process for disabling staff user-accounts when the account holder has left University employment or transferred to a different faculty, or school or department outside of their domain.

2.6.3 **Closure of Central Accounts**

The central IT accounts of paid members of staff will be lapsed by IT Username Administration when they no longer appear on SAP payroll.

It is the responsibility of schools and departments to notify IT Username Administration when the central IT accounts of visitors, etc. (i.e. the accounts of individuals who are not on SAP payroll) are required to be lapsed.

2.6.4 **Disabling of Central IT Accounts**

IT Username Administration will disable the central IT staff accounts only when requested to do so by the correct University authority\(^1\). Accounts that are disabled will remain 'locked' until the correct University authority informs IT Username Administration that they can be reinstated.

---

\(^1\) The Secretary to the University, Deputy Secretary, Director or Deputy Director HR, the University’s Legal Advisor, the Director IT or a member of the IT Security Team acting on behalf of such authority.
2.7. Student Account Management

2.7.1 Transition to Alumni Accounts
Undergraduate accounts will be transitioned into Alumni accounts 60 days after completion of their course. Taught postgraduate accounts will be transitioned into Alumni accounts 90 after completion of their course. The transition of student accounts to Alumni will disable access to University email accounts.

2.7.2 Appeals
Student accounts will remain active when IT Username Administration receives notification from the Head of Student Complaints and Appeals that an appeal has been granted. These accounts will only be transitioned to Alumni accounts when notified by the Head of Student Complaints and Appeals that the appeal has been resolved.

3. Use of Accounts

3.1. Account Restrictions
You may only use computer accounts that you have been officially authorised to use. Using a computer for which you have not been given permission to use can constitute a criminal offence under the Computer Misuse Act 1990.

Account holders must not divulge their logon credentials to anyone else or allow any other person to use their computer account at any time, regardless of whether the other person is a member of the University. The only exception to this requirement is that logon credentials are to be divulged to the University IT Security Team when undertaking an official University investigation in accordance with the University’s Security Incident & Computer Misuse Policy.

Any misuse of a computer account may be attributed to the account holder in the first instance.

3.2. Access Parameters
In accordance with the Use of Computer Systems Policy users must not attempt to access systems, applications or data which their user account does not naturally provide access to and for which they have not been granted specific permission.

4. Controlling Shared and Other Accounts

4.1. Shared Access and Project Accounts
Project accounts and temporary accounts are permitted when justified providing ownership of and responsibility for each account is delegated to a specific individual. Temporary accounts are not to be issued until each new user signs a form to confirm that they will abide by the Use of Computer Systems Policy.

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.
4.2. **Conference and Visitors’ Accounts**

Where conference and visitor user-accounts are used a custodian in the respective school/department is to be designated as owner of the accounts and is responsible for their security, allocation and lapsing.

User-accounts are only to be issued to conference delegates and visitors when the intended recipients have signed a copy of 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 IT security staff on request.

User-account custodians are responsible for notifying IT Username Administration of the lapse date requirements 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.

5. **Third Party Access to Email and File Stores**

5.1. **Allowing Others to Access Your Email**

Members of staff 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.

5.2. **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.

5.3. **Third Party Cover Arrangements for Known Absence of Staff**

When a school or department knows that a member of staff is going to be absent from work, and that for operation reasons access will be required to either their email account or file store during their absence, they are to make arrangements in advance of the absence in accordance with 5.1 and/or 5.2 above as appropriate.

5.4. **Management Third Party Access to Email and Data**

All third party access to other users’ data in their absence must be justified for operational purposes and fully accountable. The processes for gaining third party access to a user account are defined in the Access Control and Account Management Standard.

5.5. **Third Party Access during Unexpected Staff Absence**

Where a member of staff is unexpectedly absent from work and it was not practical for advanced access arrangements to be made before their absence (see 5.3) IT will, on the correct authority, facilitate third party access to the required DS or Admin email account or file store.

On signing the third party access application form management and staff agree to adhere to the terms and conditions of access.
5.6. Approval and Authority - Third Party Access during Unexpected Staff Absence

Approval for third party access to an account when a member of staff is unexpectedly absent from work must be provided by the head of school / head of service for applications from within their respective domain.

If a head of school requires personal third party access to the data of one of their staff, the application form must be authorised by the dean of faculty.2

If a head of service or dean of faculty requiring third party access to the account of one of their staff, the application must be approved by the Secretary of the University, or in his absence, the Deputy Secretary.

Following approval of the application the Director IT, or in his absence a member for the IT Senior Management Team, must provide authority before IT staff facilitate the required access.

Third party access to IT staff accounts can only be granted when the application form has been signed by the Finance Director, or in her absence, the Secretary to the University or the Deputy Secretary.

Completed application forms will be retained by IT Username Administration for a period of two years and will be made available to auditors or the IT Security Team on demand.

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

Access will be granted to the emails or data of a former employee when requested by the respective head of school or head of service.

IT staff will only recover data associated with the subject specified, by using a search facility, and will not include any data that appears to be personal, private or confidential to the account holder.

5.8. Third Party Restrictions

Anyone who is granted operational access to another users' data may only view material that it is considered necessary to see for the operational reason for which access was granted. They are required to treat all material as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. In addition, they must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters. On signing the ‘Third Party Computer Account Access Form’ the person who is to be provided with the access to another users’ account is certifying that they have read and understood the requirements.

5.9. Control and Accountability of Student Accounts

Access to students’ files must be restricted to bone-fide reasons, such as, investigating plagiarism or malpractice, providing access to a specific file for cover staff when a normal member of staff is unexpectedly absent, or to verify that existing work space is not being used for the storage of non-work related material where more disk space is requested. If there is any

---

2 If the dean of faculty is absent, applications can be approved by the Secretary to the University, or in his absence, the Deputy Secretary.
doubt as to whether access to a student’s files is bone-fide, the head of the school is to be requested to provide the required authority.

Any person viewing a student’s accounts must do so in the presence of a second person e.g. a lecturer with a member of IT staff, or two IT staff. A written summary as to why this was done and what the outcomes were must be produced and a copy of this is to be given to the student as well as being kept on their file.

6. Dealing with Misuse, Abuse and Illegal Activity

6.1. Requests for Account Access by the Police and Law Enforcement Agencies

All requests from the police and other law enforcement agencies for access to computer information or user accounts must be directed to the Secretary to the University or in his absence, the Deputy Secretary or University Legal Advisor in accordance with the Security Incident and Computer Misuse Policy.