Sheffield Hallam University

Access Control and Account Management Policy

Issuing Authority:	Leon Etherington, Acting Chief Information Officer Information Systems and Technology
Signed:	
Date Effective:	March 2016
Review date:	February 2018
Version:	2016.2

Access Control and Account Management Policy

Objective

To control access to information and ensure that access rights to information systems are appropriately authorised and allocated.

Policy Requirements

Student Accounts

1. User accounts shall be created for students as soon as they have accepted a place on a programme of study and are regarded as provisionally enrolled. Their accounts will give them access to the University IT services, including Filestore, email account, and student portal.
2. All student users are bound by the University ***Regulations for the use of IT Facilities.***
3. User accounts shall be deleted:
    - after the end of a programme of study, however limited access to certain systems may be granted until conferment.
    - if the student is withdrawn from their course of study.
4. User accounts for a student may be disabled, or restricted:
    - if fees have not been paid
    - for disciplinary reasons
    - if their user account is known to have been compromised to protect the user and University
5. Students should change their initial password at the earliest opportunity and are strongly recommended to change their password regularly.
6. Usernames and passwords must not be shared with anyone including IS&T.
7. Students on very short courses or visits may use temporary user accounts. IT Help shall be responsible for maintaining a log of who and when the temporary account was issued to for accountability and to adhere to the University IT Regulations.

Staff Accounts

8. All staff shall have individual accounts, for privacy and accountability.
9. All users are bound by the ***Regulations for the use of IT Facilities*** and the ***JANET Acceptable Use Policy***.
10. A user account for a member of staff to use the University IT Services will be created at the request of a line manager or of an equivalent member of staff. Visiting Lecturers will be treated as employees of the University for this purpose. A record will be kept of all user accounts.
11. Access to any other restricted information system may be granted with the permission of the owner of the system. The requirement to access specific systems and content must be requested with the authority of the user's line manager. A record will be kept of all users granted access to specific systems.
12. Staff who change roles within the University require a change of role request submitted by their new line manager for new access to systems, and their old line manager to remove access from systems no longer required.

13. Users shall not allow any other person to access any system with their login details or system permissions.
14. Users shall not use the login details of another user and shall not attempt to access any systems or data for which they have not been granted permission.
15. Users shall be required to change their password in line with the current University Password Policy.
16. Accounts shall be disabled as soon as the user has left the employment of the University, or is no longer a member of the University community, unless participation in on-going projects requires access to University systems. Extending access to accounts, or specific services must be approved by either a line manager or a senior manager in a Faculty or Directorate.

Shared Accounts

17. User accounts for access to the University's IT services shall be created for individual users, and shall not be shared.
18. In cases where a generic or role-based username is required a shared account may be created, but only used for specific purposes. To ensure accountability, logs should be maintained identifying individual users for traceability purposes.

Visitors

19. Visitors who require access to University systems may use a temporary user account that will be allocated by IT Help and they will maintain a log of who and when the temporary account was issued to for accountability.
20. Access to the University Guest Wi-Fi network can also be obtained by contacting ITHelp@shu.ac.uk for a user code.
21. All visitors are bound by the ***Regulations for the use of IT Facilities*** and the ***JANET Acceptable Use Policy***.
22. Visitors who are under the age of eighteen also require a written undertaking of legal responsibility from their parent or guardian before they are given access to the University IT Services.

Misuse and Abuse

23. All instances of misuse or abuse of University IT systems, actual or perceived, shall be reported as soon as possible to ITHelp@shu.ac.uk (ext 3333) and subsequently to the Director of IS&T.
24. All investigations into computer misuse or abuse shall be conducted using the University Problem Resolution Framework, and records of the investigation kept, according to the best practice guidelines provided by: ***HEIDS/J-LIS inappropriate use investigation process***