Sheffield Hallam University

# Password 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

# Password Policy

## Objective

The University is committed to ensuring that IT systems are secure and University data and systems are only accessed by authorised users.

## Policy

All University systems enforcing password restricted access must implement the following password rules where systems support them.

- All passwords must be of a minimum length of 8 characters
- Password must contain characters from at least three of the following four categories:
    - Lowercase letters a to z
    - Uppercase letters A to Z
    - Numbers 0 to 9
    - Special characters ! # $ % ' ( ) + ? @ [ ] ^ _ { } ~ -
- Passwords must not contain any characters that are not listed above, including space characters
- Passwords must not contain the user's first name, surname or logon code and for students, also their student number.
- The previous 8 passwords cannot be re-used.
- Staff passwords will expire after 84 days by default or less depending on contractual requirements of some third parties.
- Six attempts to login with an incorrect password within 30 minutes will lock the account. Lockouts will automatically expire after 30 minutes.

All exceptions to this policy e.g. for technical systems reasons or if different levels of password security are required to meet contractual obligations, must be documented and approved by the relevant Head of Service and Director of IS&T.

## Scope

This policy applies to all staff, students, data processors, partners, suppliers and contractors and other authorised users. The policy applies to secure access to all the University's IT systems, which should where possible use the University's standard directories for authentication. Where this is not possible they should implement this policy within their own system. As above, any exceptions for technical reasons must be documented and approved.

## Implementation, guidance and good practice

Guidance and good practice on setting passwords for staff will be published on the IS&T Intranet site. Students are recommended to visit the password change web site.