1. Introduction
This policy will define how the University utilises and manages passwords to ensure the security of University devices and IT systems and services. It includes appropriate technical and procedural controls to reduce risk and meet the requirements of other University IT Security Policies.

2. Scope
2.1. This policy applies to the 'Universal' Password which is the password used by staff and students when accessing University supported equipment and IT systems and services.

2.2. Where possible all passwords should adhere to this policy but in practice this policy does not apply to some specialist passwords which are in use within the University for administrative purposes.

3. Nature of Password Complexity

3.1. Minimum Password Length - Passwords must contain at least 8 characters.

3.2. Character Variation - Passwords must contain at least:

3.2.1. One upper case character

3.2.2. One lower case character

3.2.3. One number

4. Password Uniqueness

4.1. Your Password cannot include any part of your names (i.e. JohnSmith123), or your CompID.

4.2. The previous 8 passwords cannot be re-used.

5. Password Lifecycle

5.1. Minimum Age of Password - the password cannot be changed again by the User within 5 days

5.2. Maximum age of password - the password will expire after 180 days and the user offered a chance to change it before this time.

5.3. Should the password expire for any reason assistance may be obtained from the relevant IT help location.
6. Password Lockout

6.1. The system will Lockout a user after 10 incorrect attempts to their PC Login or Staff Email accounts within 3 minutes.

6.2. The Lockout duration will be 3 minutes after which time the account will automatically be unlocked.

7. Password Reset

7.1. For more details on authentication/password management please refer to the User Management Policy.

8. Password Safeguarding

8.1. Users will not share their password with anyone else including IT Services.

8.2. Users should not use the same password across users and administrator accounts.

8.3. If the user’s password has been compromised they should change it immediately and report to IT Services

9. Document Approval

Approved by: Information Governance Steering Group

Approved Date: 19th Dec 2013

Review Date: January 2017

Reviewer: Information Governance Steering Group

10. Document History

31/07/13 A Orde, R Cross, S Buckman – Version 1
15/08/14 R Cross – Name Change update – Version 2
19/10/15 S Buckman – PREVENT and IT Services update – Version 3
19/01/16 A Orde – Annual Review – Version 4
21/06/17 M Page – Annual Review and update – Version 5