IT Acceptable Use Policy
Password Procedure

Effective Date: December 2020
Supersedes: August 2020
Last Review: January 2023
Next Review: January 2026

---

1. Definitions

Standard account	These are user-level accounts and are the most common. They provide standard access to systems to enable staff to do their job and students to pursue their studies
System level account	These are privileged user accounts and have elevated permissions to a number of systems and/or databases Examples of system level user accounts are: • "Administrator" • "Superuser" • "SA" • "root".
Service account	Service accounts are a special user account that an application or service uses to interact with the operating system and system services such as web servers, mail transport agents, databases etc. These accounts are not assigned to people.

2. Password construction requirements

2.1 The following sections provide the minimum required password construction considerations for account passwords. Where conforming to the following requirements is not possible due to limitations within the host system or application, passwords should be designed to meet as many of the requirements as possible and alternative methods of protecting the account should be employed by, for example:

- Increasing the number of characters used
- Changing the password more frequently
- Using as many different types of characters as possible

See the IT guidance pages for more information about best practice for password construction.

2.2 First time use passwords need to be forced to be changed immediately by the user, after the first use.

3. Standard Account Password Construction

3.1 All user-level passwords must conform to the following construction guidelines:

- Passwords must have a minimum of **12 characters**
- The password complexity must contain a minimum of:
    - One lowercase character
    - One uppercase character
    - One numerical character

Please note: using "space" **| : & $ ' ** can give problems with some university applications.

3.2 Passwords for Standard Accounts must be changed at least once annually. It is highly recommended that the same password is not used on multiple systems. Wherever possible, systems will be configured to alert the user of the need to change their password in advance of expiry. See here for more information about Self-Service password management.

4. System Level Account Password Construction

4.1 All system-level passwords must conform to the following construction guidelines:

- Passwords must have a minimum of **15 characters**
- The password complexity must contain a minimum of:
    - One lowercase character
    - One uppercase character
    - One numerical character
    - One special character e.g. **!"£$@%^ &*()_+**

Please note: using "space" **| : & $ ' ** can give problems with some university applications.

4.2 All system level account passwords must be changed on a regular basis, at least every 6 months and/or as part of an application upgrade. Changes must be made through the change control process.

5. Service Account Password Construction

5.1 These special user accounts use the same password creation rules as stated above for system level accounts.

6. Password Blacklisting

6.1 A blacklist is a list of words disallowed as user passwords due to their commonplace use. An individual's name, surname, username, K number are disallowed for Active Directory account passwords.

7. Account Monitoring

7.1 The password system is configured so that a user only has a limited number of attempts to enter the correct password before the account is locked out for a set period of time.

7.2 All King's accounts are subject to the following configuration:

- Internal access – 20 attempts before account is locked
- External access – 15 attempts before account is locked
- Accounts are locked out for 15 minutes before a user can attempt to log in again
- Accounts are monitored for account lock outs and Denial of Service (DoS) attacks. If an account is locked out without apparent reason or a user suffers a Denial of Service attack, the user will be advised by IT to change their password.

8. Password History

8.1 24 passwords are remembered before the first one can be reused.

9. Third Party Applications

9.1 Users are advised not to use the same password for third party applications (e.g. Dovico, TeamSeer etc)., as for systems using AD account login credentials. If the third-party account was attacked, it would leave all other accounts that use this password in a vulnerable position.

Appendix A-change log

Version	Date	Name	Role	Changes made
V3.1	21/04/23	Lauren Middlemist	IT Assurance Apprentice	Change control log added as Appendix A.
