



# Password Protection Policy

<b>Policy owner:</b> IT Services	<b>Approval date and body:</b> August 2024 - UMT
----------------------------------	--

## 1. Purpose

Passwords are the most common form of authentication used to control access to information and are an important part of University College Dublin's (UCD) efforts to protect its technology systems and information assets. This policy is designed to address password weaknesses by establishing a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Passwords are widely used because they are simple, inexpensive, and convenient mechanisms to use and implement access control. At the same time UCD acknowledges that passwords are recognized as a poor form of protection for access control on their own. For some higher-risk systems or for those with access to personal data or confidential university information, other approved authentication methods that provide higher levels of trust and accountability must be used where available.

This policy sets out University standards for:

- The creation of strong passwords
- The frequency of change and reuse of those passwords
- The protection of those passwords

## 2. Definitions

A “**strong**” password is one which has the following characteristics:

- Password is unique.
- Contains at least 10 alphanumeric characters.
  - Password must include at least one letter.
- Includes at least two of the following characteristics
  1. Contains both uppercase and lowercase letters.
  2. Contains at least one number (for example, 0-9).
  3. Contains at least one symbol or special character (for example !\$%^&\*()\_+|~-=?<>.)

A “**weak**” password is one which has the following characteristics:

- Contains less than 10 characters
- The password has been used elsewhere on a UCD or non-UCD application.
- Can be found in a dictionary, including foreign language, or exist in language slang, dialect, or jargon.
- Has been discovered in a data breach commonly known as a broken password.

- Contains personal information such as birth dates, addresses, sports teams, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contains work-related information such as building names, system commands, sites, companies, hardware or software.
- Contains a number, letter or keyboard pattern such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contains common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Is some version of “Welcome123” “Password123” “Changeme123” “L3tm31n”

Personal Data consists of:

- Any information concerning or relating to a living person who is either identified or identifiable. An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Confidential University Information consists of:

- Information which, if disclosed, deleted, altered or made publicly available could cause damage or distress to individuals, damage commercial or financial interests of the University and its connected companies, or result in the loss of intellectual property of the University or those connected to it.

### **3. Scope**

All members of UCD’s student, faculty and staff population as well as all contractors and temporary staff who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides on the University network, has access to the University network, stores any non-public University information or has been authorised as a University service including but not limited to public and private cloud services.

## **4. Principles**

### **4.1 Password creation**

- All user-level and system-level passwords, including privileged accounts, must conform to standards of a ‘strong’ password.
- All user-level and system-level passwords, including privileged accounts, must not have any of the characteristics of a ‘weak’ password.
- University passwords must be unique to University systems. Users must use a separate password for all non-University systems, for example use a different password for websites and applications (including mobile apps) such as LinkedIn, Facebook, social media sites and applications, online shopping accounts, online personal memberships and so on.
- Where possible, user accounts that have system-level privileges or administration privileges must use a unique password from all other accounts held by that user.

## 4.2 Password change

- All passwords must be changed if there is thought to be risk to UCD data because:
  - The password does not conform to standards of a 'strong' password.
  - There is suspicion that an account has been compromised.
- All passwords including system level passwords should be changed at regular intervals, ideally at least every 12 months.

For help on creating strong passwords, please search the [IT Support Hub](#) for creating "Strong Passwords".

## 5. Roles and responsibilities

### 5.1 Password protection responsibilities for users

- University passwords must be treated as sensitive, confidential University information.
- University passwords must not be shared with anyone including IT Services, administrative assistants, secretaries, managers, co-workers while on leave or family members.
- Passwords cannot be reused.
- University accounts must use Multi-Factor Authentication where supported.
- University passwords must not be inserted into email messages or any other forms of electronic communication.
- University passwords must not be revealed on questionnaires or security forms.
- University passwords should not be written down or stored anywhere in your office. They must not be stored in a file, on a computer system or mobile devices (phone, tablet) or any electronic format without encryption.
- The "Remember Password" feature of applications should not be used (for example, web browsers).

### 5.2 Password Protection responsibilities for application owners

- University applications must not store passwords in clear text or in any reversible form.
- University applications must not transmit passwords in clear-text over the network.
- University applications containing personal data or confidential university information should authenticate users using UCD's supported SSO service where feasible.
- User accounts must be configured to lockout for a duration after consecutive unsuccessful login attempts.
- University applications must prevent password reuse where feasible.
- While the use of generic accounts is not recommended, if used, passwords for generic accounts must be unique, rotated frequently and stored securely only accessible to those who need it.

### 5.3 Password Compliance

There is an obligation for all users of UCD's applications or who have been issued an IT account to:

- Comply with this policy, all other relevant policies and procedures that apply to their role in the University.
- The Chief Information Officer or their nominee will have an option of verifying compliance to this policy through various methods, including but not limited to, periodic walk-throughs, system scans and internal and external audits.

- Any exception to the policy must be approved by the Chief Information Officer or their nominee in advance.
- Any user suspecting that a password may have been compromised must report the incident to the IT Services helpdesk at [www.ucd.ie/ithelp](http://www.ucd.ie/ithelp) and change all related passwords immediately.

## 6. Breaches in Policy

IT Services may withdraw services from any user or system arising from a suspected breach of this policy.

## 7. Related documents

This policy is related to the following existing University policies:

- [Acceptable Use Policy](#)
- [University Data Protection Policy](#)

The policy will conform to UCD's responsibilities under Data Protection legislation.

## 8. Version history

Name	Version	Date	Reason for issue
Paul Kennedy	1.0	Dec 2016	First edition - Password Protection Standards
Paul Kennedy	2.0	Feb 2018	Draft Password Protection Policy
Genevieve Dalton	2.1	Mar 2018	ITLG Review
Genevieve Dalton	2.2	Jul 2018	Feedback from UMT April 2018
Genevieve Daltron	2.3	Sep 2018	University Consultation Review
Phillip Fisher	2.4	Sep 2018	Policy Approved
Elaine Timmons	2.5	Oct 2022	Editorial amendments to web links
Susan Devereux	2.6	May 2024	Review by IT Security Governance Group and ITLG
Susan Devereux	2.7	June 2024	Review by UMT ITSG
Bridín Walsh	3.0	Aug 2024	Policy Approved by UMT