lwetb
Bord Oideachais agus Oiliúna an Longfoirt agus na hIarmhí
Longford and Westmeath Education and Training Board

| | |
|---|---|
| **Title** | **LWETB Password Policy** |
| **Date** | 14th September, 2020 |
| **Approved By** | Chief Executive LWETB |
| **Noted By** | LWETB Board |

# LWETB
# Password Policy

## Purpose

Passwords are an important part of LWETB's efforts to protect its technology systems and information assets by ensuring that only approved "Users" can access these systems and assets.

LWETB recognises, however, that passwords have weaknesses as an access control. For higher risk systems, other approved authentication methods that provide higher levels of trust and accountability than passwords may be used.

However, many of LWETB's systems continue to rely on passwords alone. This policy is designed to address their weaknesses by establishing best practices for the composition, lifetime and general usage of passwords.

LWETB may supplement or modify this policy for users in certain roles. This Password Policy complements similar LWETB policies, such as the Technology Acceptable Usage Policy. A comprehensive list of ICT policies may be located in the ICT Policy Framework.

## Scope

This policy applies to all approved "Users" of LWETB's systems, information and I.T. resources. Individuals covered by the policy include (but are not limited to) [employees (both full and part time), contractors, interns, partners and / or consultants, external individuals and organisations here on in to be referred to as "Users"]

## Policy Schema

### Password Confidentiality

A password can provide effective authentication if and only if it is known only to the individual user. Users must ensure the confidentiality of their passwords at all times. System developers and administrators will ensure that systems do not store passwords in clear text.

Administrative processes may necessitate temporary exceptions to this principle, but these will be kept to an absolute minimum.

### Password Construction

Password length and complexity requirements provide resistance to common kinds of attacks. As a result of technology constraints, password construction rules may vary from one system to another, but they will meet (or exceed) these requirements wherever possible.

LWETB's recognises that long and complex passwords may be difficult for users to remember, and thus, this policy provides guidance to end users on how to construct a memorable password that meets (or exceeds) these requirements.

## Password Construction Rules

A password must be made up of:

- [8] or more characters
- At least [1] uppercase letter
- At least [1] lowercase letter
- At least [1] digit (0 through 9) or special character ($, @, # and so on)

Note: These rules are enforceable on all systems under direct LWETB control.

A password must not include:

- The user's user ID
- The name of the group which the user account belongs to

A password ideally should not include anything that is meaningful to the user, such as a name, a date (such as birthdays and anniversaries), telephone numbers, postal codes and car registration numbers.

## Password Change and Reuse

Users will be forced to change their passwords every sixty days in order to minimise the window of opportunity for an attacker who has discovered a user's password. Where the system does not allow for user initiated changes, [LWETB ICT Staff or LWETB designated appointees] reserve the right to change these passwords as required. These password changes will be communicated to relevant system users.

A user's new password must be substantially different from any recently used password, for example:

Old Password: ILoverealityTV!

Bad New Password: ILoverealityTV123!

Better Potential Password: RealityTV!is#Finished2020

A user is free to choose a new password at any time on certain systems. However, performing multiple changes in quick succession to enable continued use of a recently used password is prohibited.

## Users' Responsibilities

If you are a user of LWETB's systems, you have the following responsibilities regarding the password you use on any of LWETB's systems.

These responsibilities apply even if the system does not enforce any specified rules:

a) You must keep your password confidential at all times.

b) You must not disclose your password to anyone, including LWETB's management and technical support staff, even if they demand it.

- If this happens, you must escalate to LWETB's ICT Department immediately. The only exception is disclosure to An Garda Síochána in accordance with national laws. Such requests should be immediately directed to the appropriate Director of OSD.

- There may be certain instances where access to a specific user's account is required, for example, certified long-term illness. In these incidents, LWETB's Director of OSD will request in writing that LWETB's ICT Department reset the password.

c) You should not use any password that you use on any LWETB's systems on any external system (including Internet banking and social networking services).

d) You should not write down your password.

e) You should not use the "remember password" feature in any Web browser.

f) You must choose a password that meets or exceeds the length and complexity requirements set out in Password Construction Rules section.

Note: This is your responsibility as an end user of LWETB's IT systems, even if these rules are not enforced by a particular system. Sometimes, technical restrictions on a system do not allow you to choose a password that meets these requirements. In such systems, you are required to come as close as possible to password construction rules in the password construction rules section.

## Enforcement

This policy will be enforced by technical controls wherever feasible, as indicated in the text, e.g. in systems that support such actions, users will be prompted to change their password, within sixty days.

All users of LWETB's systems, information and I.T. resources have a responsibility to promptly report any known instances of noncompliance to line management or LWETB's ICT Department.

## Compliance

Individuals found to be in breach of this Password Policy, may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there may be a case to answer by an Employee / User, the matter will be referred into the appropriate stage of the relevant disciplinary procedure as appropriate to that Employee / User.

For the avoidance of doubt, where questions remain as to what constitutes "appropriate use", contact LWETB's ICT Department for full clarification.

## Tips for Choosing a Good Password (Advisory)

The length and complexity requirements may appear to make it hard to choose a password that is easy to remember, but it can be pretty straightforward to do so.

A password that meets the minimum length requirement must be rather complex. You can readily construct such a password from the initial letters of a favorite quotation, song lyric, poem and so on, capitalising some letters, and substituting a number or special character in an appropriate place.

For example:

- Ww1dwyga — What would I do without your great attitude?
- Itwbtd2S — In the week before their departure to Spain.

A "very long" password can be relatively simpler. Choose three simple words, capitalizing some letters, and link them with a number or special character.

For example:

- gorilla8Banana#delicious

## Related Documents

Department of Education and Skills circular on Revised Procedures for Suspension and Dismissal of Teachers and Principals (ETBs)

Department of Education and Skills circular on procedures for Suspension and Dismissal of Principals of Community National Schools

ETBI & Unions Consultative Forum - Disciplinary Procedure for staff employed by Education & Training Boards

Procedures for principals relating to their work, conduct and matters of professional competence in their role as principals

## Responsibilities

| Owner | Responsibilities |
|---|---|
| Director of Organisation Support and Development | Revisions and updates to the Policy |
| LWETB Senior Leadership Team | Review of the Policy |
| LWETB Chief Executive | Approval of the Policy |
| LWETB Board | Noting of the Policy |