



# Password Policy

<b>Approved by:</b>	Brian McGorry	<b>Date:</b> 01/09/2025
<b>Last reviewed on:</b>	01/09/2025	
<b>Next review due by:</b>	31/08/2026	
<b>Version control:</b>	V1	

### **Purpose**

This policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

### **Scope**

This policy applies to passwords for the use of all IT services administered by the Fowler Education Football Academy (FEFA), including services provided under contract for FEFA.

This policy does not apply to privileged accounts such as network and system service accounts, which do not belong to a nominated individual but are necessary for the automated operation of the network, applications and connected services.

### **Policy Statement**

The information system resources are assets important to FEFA's business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is the College's policy that appropriate access control measures are implemented to protect its information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

Passwords are a key element of access control and require effective management in order to ensure that the College's IT assets are not compromised by unauthorised access.

### **Policy Objectives**

The objectives of this policy with regard to the protection of information system resources against unauthorised access are to:

- Minimise the threat of accidental, unauthorised or inappropriate access to electronic information owned by FEFA or temporarily entrusted to it;
- Minimise the network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources;
- Minimise reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality; and
- Raise awareness of the factors which either weaken or strengthen passwords to ensure that passwords of an appropriate strength are in use.

### **Policy Overview**

This policy sets out the rules, requirements and guidelines covering the management of passwords. Passwords are important because they provide entry to FEFA's IT resources.

Passwords play an important role in the defence against malicious misuse of these resources. Any misuse of Passwords could result in the confidentiality, integrity or availability of vital information being compromised or FEFA being held responsible for illegal activities.

### **Policy Requirements**

Responsibilities

- All Users are responsible for ensuring that this Policy is complied with.
- All Users are responsible for maintaining Password security in accordance with this Policy in all of their activities.

- Any User who for any reason has gained temporary or permanent knowledge or use of a password relating to any part of an information system for which they do not normally have access should identify this to the IT Team immediately, so that the situation can be rectified.

### **Password Characteristics**

Passwords are used for various purposes; best practice dictates that user passwords should be described as either 'complex' or 'strong'.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&\*()\_+|~=-\`{ } [ ] : ; ' < > ? , . /
- Are at least eight alphanumeric characters long for normal user accounts
- Are at least fifteen alphanumeric characters long for administrator (high privilege) and system service accounts

### **Password History**

Passwords should not be reused. A password should not be the same as the one used during the past 5 changes.

### **Password Expiry**

- Student passwords do not expire, however any student who needs their network login password changed can change it themselves by logging on to a computer or visiting the IT Team.
- The College directory system requires employees to change their network login password every 90 Days, also on first use if the employee is a new user.

### **Password Security**

- The purpose of passwords is to protect the confidentiality and integrity of FEFA IT facilities and assets. The combination of a particular user name and password also provides an audit trail identifying which particular authorised user accessed a resource at a particular time.
- IT Services will disable any accounts identified as having shared passwords, and makes the following recommendations to users as password best practices.
- Passwords must not be shared with anyone, including the IT Team. All passwords are to be treated as sensitive and confidential information.
- Two factor authentications for Office 365 is in place.

### **Users are expected to observe the following:**

- Do not e-mail or otherwise communicate your password to anyone
- Do not reveal a password over the phone to anyone
- Do not write a password down or store it on your computer in a format readable by others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- Do not use the "Remember Password" feature of applications and websites
- Do not share a password with family members
- Do not reveal a password to co-workers while on leave
- Do not include personal details which may be readily known to others (e.g. your partner's name, your birthday, names of pets, and similar)
- Don't use common sequences of numbers or letters (e.g. 12345678 or qwerty, etc.).

- When leaving the desk to ensure the User 'logs off' the computer or if the computer is not shared with other users that it is 'locked'.

### **Reporting Security Incidents**

All security incidents, including actual or potential unauthorised access to the College's IT systems, should be reported immediately to the IT Team.

These incidents include occasions when:

- A password may have been accidentally revealed.
- It is suspected that access has been gained to a system by an unauthorised person.

### **Disciplinary Process**

The Fowler Education Football Academy reserves the right to audit compliance with the Policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the organisation's Disciplinary Policy.

### **Deviations from Policy**

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Assistant Principal, in the first instance.