Access Control Procedure

Full Council Approved:	3 June 2026
Last Reviewed:	June 2026
Due for next Review:	June 2029

1. Purpose

The purpose of this policy is to implement strong access control measures across Fleet Town Council's network, information systems and premises. This will provide appropriate, authorised, and auditable user access control, whilst ensuring the confidentiality, integrity, and availability of information.

2. Scope

The scope of this policy applies to all Fleet Town Council employees, Councillors, customers, vendors, and anyone else with any form of access to Fleet Town Council information, information systems and premises.

3. Responsibilities

The Executive Officer is responsible for:

- Creating, documenting, and maintaining individual user/user group profiles that meet the requirements of the Access Control Policy.
- The administration of allocated and authorised user/user group access rights in conformity with the policy.
- The initiation and administration of new and changed user access requests and user training.
- Authorising access requests, in line with business and security policies and procedures.
- Reviewing user access rights.

Asset owners are responsible for authorising access requests to their information assets in line with conformity to the security requirements of the asset.

4. Access Control Policy

The control of access to Fleet Town Councils information assets is a fundamental part of a defence in depth strategy to information security. If Fleet Town Council is to effectively protect the confidentiality, integrity, and availability of classified data then a comprehensive mix of physical and logical controls must be in place.

Fleet Town Council's policy regarding access control must ensure that the measures implemented are appropriate to the council requirements for protection and are not unnecessarily strict. The policy therefore must be based upon a clear

understanding of the council requirements as specified by the owners of the assets involved. These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service.
- Relevant legislation that may apply such as the Data Protection Act / General Data Protection Regulation (GDPR).
- The regulatory framework in which the council and the system operate.
- Contractual obligations with external third parties.
- The threats, vulnerabilities and risks involved.
- The council's appetite for risk.

This Access Control Policy is designed to consider the council and information security requirements of Fleet Town Council and is subject to regular review to ensure that it remains appropriate.

This control applies to all systems, people and processes that constitute the council's information systems, including councillors, employees, suppliers and other third parties who have access to Fleet Town Councils systems.

5. Access To Networks And Network Services

The use of non-council owned devices connected to Fleet Town Council's network can seriously compromise the security of the network. Specific approval must be obtained from the Executive Officer and IT Helpdesk (Cloudy IT) before connecting any equipment to the council's network.

A policy of using two factor authentication for remote access should be used in line with the principle of "something you have and something you know" to reduce the risk of unauthorised access from the Internet.

Council/Business Partners or 3rd party suppliers must not be given details of how to access the Fleet Town Council's network without permission from the Executive Officer. Any changes to supplier connections, such as on termination of a contract, must be immediately sent to the Executive Officer so access can be updated or terminated. All permissions and access methods must be controlled by the Executive Officer.

Council/Business Partners or 3rd party suppliers who require access to the network must contact the relevant Line Manager in the first instance. Line Managers must then contact the Executive Officer. A log of activity will be maintained via Office 365 and Windows Audit logs. Remote access software and user accounts must be disabled when not in use.

6. User Registration, De-Registration And Access Provisioning

A request for access to Fleet Town Councils network and systems must first be submitted to the Executive Officer, for approval. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account will have a unique username that is not shared with any other user and is associated with a specific individual and not by role or job title.

Generic user accounts should not be created as they provide insufficient allocation of responsibility.
An initial strong password should be created on account setup and communicated to the user via secure means. The user is required to change this password on first use of the account.

When an employee leaves Fleet Town Council under normal circumstances, their access to systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the Executive Officer.

In exceptional circumstances, where there is perceived to be a risk that the employee may take action that may harm Fleet Town Council prior to, or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution should especially apply in the case where the individual concerned has privileged access rights, such as domain admin.

User accounts should be initially suspended or disabled only and not deleted. User account names should not be reused as this may cause confusion in the event of a later investigation.

User reports provide detailed information on inactive accounts, which are suspended after 30 days automatically and require re-activation by the Executive Officer should they still be required.

Each user must be allocated access rights and permissions to systems and data that are commensurate with the tasks they are expected to perform. Typically, this should be role-based. Group roles should be maintained in line with council requirements and any changes to them should be formally authorised and controlled via the change management process.

Additional, ad-hoc permissions should not be granted to user accounts outside of the group role. If such permissions are required, this should be addressed as a change and formally requested.

7. Management Of Privileged Access Rights

Privileged access rights, such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users, such as IT support staff should not make day to day use of user accounts with privileged access. Separate "admin" user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual. Generic admin accounts should not be used as they provide insufficient identification of the user.

Vendor provided systems must have initial passwords changed from default to complex passwords that should only be accessed by users with Privileged Access Rights.

The use of user accounts with privileged access in automated routines, such as batch or interface jobs should be avoided where possible. Where this is unavoidable the password used should be protected and changed on a regular basis.

Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use. The following is the process which must be followed when granting privileged access rights, such as 'Admin' permissions:

1. Line Manager identifies requirement for privileged access rights.
2. Line Manager requests and obtains written approval from Executive Officer.
3. Executive Officer confirms approval in writing to Line Manager.
4. Line Manager makes request for privileged access rights to IT Support (Cloudy IT), providing written authorisation.

8. Management Of Secret Authentication Information Of Users

IT Support (Cloudy IT) set the initial passwords. These will be strong passwords according to the Password Policy. Passwords will be set to expire upon first logon at which point users will define new ones, which are only known to them, and which meet the parameters defined for each system.

When additional authentication tools are to be used, such as a two-factor authentication method, the appropriate procedure for the setup of these items will be followed as detailed during the guided setup procedures.

9. Review Of User Access Rights

On a regular basis, at least every six months, asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place to identify:

- Individuals who should not have access, such as leavers.
- User accounts with more access than required by the role.
- User accounts with incorrect role allocation.
- User accounts that do not provide adequate identification, such as generic or shared accounts.
- Any other issues that do not comply with this policy.

A review of user accounts with privileged access will be carried out by the Executive Officer on a quarterly basis to ensure compliance.

10. Removal Or Adjustment Of Access Rights

Where an adjustment of access rights or permissions is required, such as an individual changing role, this should be carried out as part of the role change. It should be ensured that access rights no longer required as part of the new role are removed from the user account. If a user is taking on a new role in addition to their existing one, then a new composite role should be requested. Due consideration of any issues of segregation of duties should be given.

Under no circumstances should administrators be permitted to change their own user accounts or permissions.

11. Use Of Secret Authentication Information

Users are required to follow the Council's Password Policy. Subsequently users shall be responsible for the following:

- Where access to a facility is protected by an authentication method such as a password, the user must not make it available to any other person. If they do so, they will be responsible for all the activities originating from that account.
- A user shall not use another user's account nor make any attempts to find out the password of the resource they are not entitled to use.

All users while using their account, are responsible for:

- Using their account to conduct their assigned responsibilities only.
- All activities that originate from their account.
- All information sent from, intentionally requested, solicited, or viewed from their account.
- Publicly accessible information placed on a computer using their account.
- Not revealing their account information to any other individual.

User accounts to access Council information will be given as authorised by the Executive Officer.

All users shall be responsible for maintaining the confidentiality of the password and account and shall be fully responsible for all activities that occur under their account. They shall immediately notify the Executive Officer/IT Support (Cloudy IT) of any unauthorised use of their password or account or of any other breach of security.

Users shall ensure that their passwords shall be complex even though application/information system does not enforce password complexity. This way the password security will not be completely dependent on the system.

12. Information Access Restriction

The following general principles have been used when designing access controls and restrictions for Fleet Town Council's systems and services:

- Defence in Depth – security should not depend upon any single control but be the sum of many complementary controls.
- Least Privilege – the default approach taken should be to assume that access is not required, rather than to assume that it is.
- Need to Know – access is only granted to the information required to perform a role, and no more.
- Need to Use – Users will only be able to access physical and logical facilities required for their role.

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

As part of the selection of cloud service providers specifically, the following access-related considerations should be considered:

- User registration and deregistration functions provided.
- Facilities for managing access rights to the cloud service.
- To what extent access to cloud services, cloud service functions and cloud service customer data can be controlled on an as required basis.
- Availability of multi-factor authentication for administrator accounts.
- Procedures for the allocation of secret information such as passwords.
- Storage of passwords for support purposes in highly secure, audited, and robust vaults.

Addressing these requirements will ensure that the provisions of this policy can be met in the cloud as well as within on premises systems.

13. Secure Log-On Procedures

Screens do not display any system or application identifiers until the logon has been successfully completed. The display on the logon screen includes a general notice warning that the information system should only be accessed by authorised users. The screen provides no help messages during the logon procedure.

Single Sign-On (SSO) will be used within the internal network where supported by relevant systems, unless the security requirements are deemed to be such that a further logon is required.

The system validates the logon data only on completion of input and then, if there is an error, the system requires the user to try again. The logon procedure limits the number of unsuccessful attempts allowed to five which are recorded, and the machine is locked requiring a key only obtained via the IT Support (Cloudy IT). If the unlock key is entered incorrectly the machine is wiped.

The system limits the maximum time allowed for the logon attempt to 15 minutes. When the limit is exceeded, the system terminates logon. Password characters are hidden by symbols and always encrypted before being sent across the network.

14. Multi Factor Authentication

Strong passwords are essential against unauthorised access however, a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and strong password techniques.

The Council's policy is to make use of additional authentication methods based on risk, considering:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

The use of multi-factor authentication methods should be justified based on the above factors and securely implemented and maintained where appropriate.

Whether single or multi-factor authentication is used, the quality of user passwords should be enforced in all networks and systems in accordance with the Password Policy.

15. Use Of Privileged Utility Programs

Most Operating Systems (OS) have one or more system utility program and commands that can override system and application controls. The use of such critical system utilities and OS commands shall be tightly controlled by disallowing privileged access of the OS to users who do not need it.

Segregation of utility programs from the application software is maintained and the limitation of the use of utility programs to the minimum practical number of trusted, authorised users is managed. The availability of utility programmes is limited and logged. Should utility programmes be unnecessary they are removed or disabled.

16. Access To Program Source Code

Where bespoke software development is undertaken, program source code is protected from unauthorised access. Effective version control and software configuration management procedures are implemented from the start of the development including measures for source code check in/check out.

17. Physical Access

Fleet Town Council will abide by the following physical security requirements:

- All visitors will be required to sign in at reception and will be always escorted by a member of staff.
- Access to Data centres and IT Server Rooms/Data cabinets will be restricted to only those that require access, and this must be approved by the Executive Officer.
- Physical documentation will be secured in lockable cabinets or lockable rooms when unattended.
- CCTV will be actively monitored both inside and outside of the office.
- Staff badges/passes must be always displayed.
- All entry points around the physical security perimeter are risk assessed to ensure they offer a good degree of protection with no weak points.
- An alarm system is in place and will be set when the office is unattended.
- All windows and doors must be closed and locked when the office is unattended.

18. Related Documents

- Acceptable Use Policy
- Anti-Malware Policy
- Information Security Awareness Policy
- Password Policy