Digital Information Systems Security Policy

Our responsibilities for ensuring the security of information systems at Llantwit Fardre Community Council

1 Introduction

The continued confidentiality, integrity and availability of information systems underpin the operations of Llantwit Fardre Community Council. A failure to secure information systems would jeopardise the ability of Llantwit Fardre Community Council's to fulfil its function.

The Council is committed to delivering and successfully implementing Information Security Management, but this is only possible if all staff and third parties are aware of, and carry, out their own personal responsibilities.

This Digital Information Systems Security policy provides the guiding principles and responsibilities of all members of Llantwit Fardre Community Council , its Staff and third parties required to safeguard its information systems. Other supporting policies give greater detail on specific subject areas.

1.1 Purpose of Policy

The intention of this policy is to:

- Ensure that Llantwit Fardre Community Council's information systems are protected from security threats and to mitigate risks that cannot be directly countered;
- Ensure that all Llantwit Fardre Community Council's staff and third parties are aware of and are able to comply with relevant UK and EU legislation.
- Ensure that Llantwit Fardre Community Council's staff and third parties are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access;
- Ensure that all users are aware of and comply with this and other supporting policies.
- Safeguard the reputation and business of Llantwit Fardre Community Council's by ensuring its ability to meets its legal obligations and to protect it from liability or damage through misuse of its IT facilities

- Ensure timely review of policy and procedure in response to feedback, legislation and other factors so as to improve ongoing security.

1.2 Scope

This Information Systems Security Policy applies to all Llantwit Fardre Community Council's staff and third parties who interact with Llantwit Fardre Community Council's data, the data of its Clients, and all of the systems used to store or process it.

2 Policy

2.1 Awareness and communication

All authorised users will be informed of the policy and of supporting policies and guidelines when commencing employment, contracting or subcontracting with Llantwit Fardre Community Councils . Updates will be given at the appropriate time.

2.2 Definitions

Llantwit Fardre Community Council's Data - This includes all data elements that are owned or licenced by Llantwit Fardre Community Council or any information processed by the Council on behalf of its Members.

Llantwit Fardre Community Council's information systems - This includes but is not limited to all information systems owned, held, utilised or present on the Llantwit Fardre Community Council's network, and anyone making use of them.

Data Protection Officer (Clerk) – This person is ultimately responsible for data management, retention and security.

Data Processors and Data Custodians – These persons are responsible for the use, safe custody, transport and storage of data pertaining to Llantwit Fardre Community Council's and its Members and users .

2.3 Information Security Principles

The following principles provide a framework for the security and management of Llantwit Fardre Community Council's ' information and information systems.

a) Information should be classified in line with the Information Classification Framework and in accordance with any other legislative, regulatory, or contractual requirements that might increase the sensitivity of the information and security requirements.
b) The Data Protection Officer is responsible for ensuring that data is classified and that in partnership with Data Custodians the information is treated in line with its classification level with appropriate procedures and systems in place to cater for this. Where personal data are stored, appropriate consent for storage and processing must be gathered and recorded as defined in the General Data Protection Regulation EU (GDPR) 2016/679, in force from the 25th May 2018.

c) All individuals covered by the scope of this policy must handle information appropriately in accordance with its classification level.
d) Information should be only available to those with a legitimate need for access.
e) Information will be protected against unauthorised access and processing.
f) Information will be protected against loss and corruption.
g) Information will be disposed of securely and in a timely manner with measures appropriate for its classification.
h) Breaches of policy must be reported to the Data Protection Officer and Clerk by anyone aware of the breach as soon as it is practicably possible to do so.

2.4. Legal and regulatory obligations

Llantwit Fardre Community Council's' Members staff and third parties must adhere to all current UK and EU legislation as well as regulatory and contractual requirements. A summary of the relevant legislation is included in the Llantwit Fardre Community Councils. Guide to legislation relevant to the Information Systems Security Policy.

2.5 Information Classification

The following provides a summary of the Information Classification levels which are part of the Information Security Principles.

Category - Highly Restricted

Description

Highly confidential information whose inappropriate disclosure would be likely to cause serious damage or distress to individuals and/or constitute unfair/unlawful processing of "sensitive personal data" under the Data Protection Act; and/or

Seriously damage Llantwit Fardre Community Council's ' interests and reputation; and/or significantly threaten the security/safety of Llantwit Fardre Community Council's Members' staff and third parties.

Examples

- Sensitive personal data relating to identifiable living individuals
- Individual's bank details
- Large aggregates (>1000 records) of personal data such as personal contact details
- Non-public information that facilitates protection of individuals' safety or security of key functions and assets e.g. network passwords and access codes for higher risk areas

Category - Restricted

Description

Confidential information whose inappropriate disclosure would be likely to cause a negative impact on individuals and/or constitute unfair/unlawful processing of “personal data” under the Data Protection Act; and/or damage Llantwit Fardre Community Council’s commercial interests, and/or have a negative impact on Llantwit Fardre Community Council’s reputation.

Examples

- Personal data relating to identifiable living individuals
- Staff or Client contact details
- Audit data containing detailed financial information
- Audit data relating to ongoing commercial tender processes, valuations
- Audit data relating to payroll or staffing matters

Category - Internal Use

Description

Information not considered being public which should be shared only internally but would not cause substantive damage to Llantwit Fardre Community Council’s or other individuals if disclosed.

Examples

- Non-confidential internal correspondence e.g. routine administration such as meeting bookings and catering arrangements
- Meeting minutes, internal policies and procedures

2.6 Compliance and Incident notification

It is vital that all users of information systems at Llantwit Fardre Community Council’s comply with the information security policy. Any breach of information security is a serious matter and could lead to the possible loss of confidentiality, integrity, or availability of personal or other confidential data. Such a loss may result in criminal or civil action against Llantwit Fardre Community Council’s including the loss of business and financial penalties.

Any actual or suspected breach of this policy must be notified to the Clerk and Data Protection Officer at the earliest possible opportunity. All security incidents will be

investigated, and consequent actions may follow in line with this policy; ' Llantwit Fardre Community Council's disciplinary policy; and relevant laws.

The Data Protection Officer will be informed of any breach found to affect personal data in keeping with Llantwit Fardre Community Council's Data Protection Policy. Compliance with this policy shall form part of any contract with a third party that may involve access to Llantwit Fardre Community Council's systems or data.

3. Responsibilities

3.1 Individuals

Individuals must adhere to the Acceptable Use Policy and follow relevant supporting procedures and guidance. An individual should only access systems and information they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data. In particular individuals should adhere to the information security 'dos and don'ts' outlined in the table below:

DO	**DO NOT**
Do use a strong password of at least eight digits containing alpha and numeric characters and at least one capital letter. You must change it if you think it may have been compromised, or if a software or service provider issue a security alert to do so.	Don't give your password to anyone
Do report any loss or suspected loss of data immediately to the Data Protection Officer at: Clerk@llantwitfardre.cc	Don't reuse your previous password(s) for any other account
Do be on your guard for fake emails from organisations that appear to be legitimate, i.e. Town Councils demanding you open a .PDF file or click on a link. Remember, always check the email address. Also screen phone calls requesting confidential information - report anything suspicious to the Data Protection Officer at Clerk@llantwitfardre.cc	Don't open suspicious documents or links
Do keep software up to date and use an auto-updating antivirus on all possible devices	Don't undermine the security of ' Llantwit Fardre Community Council's systems
Do be mindful of risks using public Wifi or computers	Don't access Llantwit Fardre Community Council's' Data Store, or systems using public Wi-Fi
Do ensure Llantwit Fardre Community Council's' data is stored on Llantwit Fardre Community Council's Data Store.	Do not copy confidential Llantwit Fardre Community Council's' data without permission

Do password protect your personally owned devices, preferably with thumb print access if available. Always lock your device if you are to leave it unattended on a client site.	Do not leave your computers or phones unlocked when unattended

3.2 The Data Protection Officer

The responsibilities of the Data Protection Officer

The Data Protection Officer is responsible for the maintenance, security and proper usage of all data held by Llantwit Fardre Community Council's, and for ensuring that data custodians who maintain and process Client data as part of their Auditing duties are aware of any additional requirements that are required to safeguard data above and beyond those for normal internal data.

The Data Protection Officer is also responsible for information security training, the publication of the Information Handling protocols, policy and compliance associated with the Data Protection Act and the General Data Protection Regulation EU 2016/679.

3.3 Data Custodians

Data custodians are responsible for the data stored on mobile information systems and smart devices that hold both Llantwit Fardre Community Council's own and Client data that is examined, processed, reported on and stored as a result of the Audit function. In addition to their individual responsibilities 3.1 they must:

- Ensure that the physical and network security of their system is maintained.
- Ensure that the system(s) they maintain is/are suitably configured.
- Ensure that all data is appropriately stored and backed up.
- Ensure that appropriate access controls are in place to meet the Legal requirements and those of the Data Protection Officer.
- Understand and document any data security risk of which they become aware, take suitable steps to mitigate and ensure that this is communicated to the Data Protection Officer.
- Ensure that their systems are compliant with legal and Llantwit Fardre Community Council's ' contractual requirements.

3.4 IT Security Management

The Clerk is responsible for the Electronic Information Systems Security Policy and will, from time to time, advise on appropriate security measures for any new types of information systems that are introduced in order to aid clarity of the policy.

3.5 Computing Services

Llantwit Fardre Community Council's will ensure the provision of IT infrastructure consistent with the demands of this policy and to support the Data Protection Officer, Data Custodians and Data Processors.

3.6 Internal Data Audit

Llantwit Fardre Community Council's will conduct an annual Internal Data Audit across its digital estate to ensure, as far as it is reasonably possible to do so, that all Staff, Contractors, Sub-Contractors and Consultants abide by the Company's policies and that the Company is fully compliant with current Data Protection regulations and legislation.

4. Supporting regulations, policies, and guidelines

Other policies issued by Llantwit Fardre Community Council's support and reinforce this policy statement. These include but are not limited to:

- Data Protection Policy & General Data Protection Regulation
- Information Classification Framework and handling protocol
- Acceptable Use Policy

Policy review

Llantwit Fardre Community Council's will review this policy when required to ensure that it remains appropriate and up to date. Any questions or concerns should be made to the Data Protection Officer Clerk@llantwitfardre.cc

Document Control Information

Owner	
Version Number	V 1.0
Original approval date	10.02.25
Approved By	Finance & Policy Committee
Date of last review	10.02.25
Date of next review	February 2026