EGERTON PARISH COUNCIL

INFORMATION SECURITY POLICY

1. Introduction
Egerton Parish Council recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. The Council believes that the security of information is essential.
The policy below is to protect all **information assets owned** and used by Egerton Parish Council (EPC).
This policy includes recommendations contained in ISO 27001 (previously British Standard 7799) – A Code of Practice for Information Security Management.

2. Definition
Information Security is defined as the preservation of:

- **Confidentiality**: protecting information from unauthorised access and disclosure;
- **Integrity**: safeguarding its accuracy and completeness; and
- **Availability**: ensuring that information is available to authorised users when required.

Information exists in many forms. It may be on paper, stored electronically, transmitted over a network, viewed in videos or films, or spoken in conversation. Whatever its form, or medium, appropriate protection is required to ensure the Council can continue to operate, perform its duties and to avoid breaches of the law, statutory, regulatory or contractual obligations.

3. Privacy of Information
It should be noted that EPC is a public body and will seek to carry out its business in a public and transparent way. Much of its business is conducted in meetings open to the public. All information given at a public meeting of EPC is in the public domain, is likely to appear in the minutes and may be reported by the press. The Council publishes many of its documents on its website.
Although the Council owns some IT equipment, this is limited and much business (principally by email) is conducted on Councillors' personal devices.

4. Protection of Personal Information
The Council may hold and use information about employees, councillors, members of the public, and other data subjects for essential administrative and business purposes. When handling such information, the Council, must comply with the Data Protection Principles which are set out in General Data Protection Regulation (GDPR).

Responsibilities under current law are set out in the Council's Data Protection Policy.

5. Responsibility for Information Security
Information security is the responsibility of all Councillors, Committees and sub committees of EPC,employees (temporary or permanent), contractors, agents and anyone else processing information on our behalf. Every person handling information or using Council IT equipment is expected to observe the information security policies and

procedures, both during and, where appropriate, after his or her time at the Council. Councillors should have no expectation of privacy in their use of any EPC business system. Any correspondence, documents, records or handwritten notes, may be disclosable to the public, under the Freedom of Information Act 2000 or the Data Protection legislation. Any comments recorded or notes written must therefore be appropriate.

6. Compliance with Legal and Contractual Requirements
6.1 Use of EPC equipment
Where Council IT facilities are provided they must only be used for authorised purposes. Limited personal use is permitted.

6.2 Use of Personal equipment
Councillors and staff conducting Council business on their own personal equipment have a responsibility to follow established Good Practice to protect against malicious software and unauthorised external access to networks and systems. Information should be regularly backed up. EPC software should not be copied without authority, nor should copies of EPC information be made for personal use.

6.3 Access to EPC Information
Although the privacy of users' own files will be respected the Council must reserve the right to examine systems, directories, files and their contents, on personal equipment e.g. personal computers, laptops, iPads and mobile phones. This is to ensure compliance with the legal and statutory regulations.
Authorisation for access must be obtained from the Clerk, or the Chair. Access shall be limited to the least action necessary to resolve the situation.

7. Social Media and Online Participation
This policy includes Social Media and Online Participation, i.e. forums, blogs, websites and so on. Councillors and staff should not disclose personal information about EPC's staff, Councillors or business online, unless expressly authorised to do so.
Councillors using social media should always be aware of their association with the Council and ensure that their posting is consistent with this.
Councillors are personally responsible and liable for the content they publish. They should be mindful that posts might remain public indefinitely.

8. Retention and Disposal of Information
All Councillors and staff have a responsibility to consider security when disposing of information in whatever medium and format it is kept.

The Council's Data Retention policy provides guidance on retention periods.

Specifically, all personal information shall only be retained for no longer than is necessary to complete the Councils business and should then be destroyed in line with the guidelines laid out in the Data Retention Policy

9. Reporting
All staff and Councillors should report immediately to the Clerk, or to the Chair;

- any observed or suspected security incidents where a breach of the Council's security policies has occurred;
- any security weaknesses in, or threats to, systems or services; and

- any Software malfunctions