Over Parish Council Information Security Policy

1. OBJECTIVE

Information plays a fundamental role in supporting all activities of the Council. Properly securing all information that Council processes is essential to the success of its administrative activities. This is to be achieved through managing the three essential attributes of information security: Confidentiality, Integrity and Availability, which are the vital building blocks for safeguarding Council's information.

The objectives of this policy are to:

- Enable adequate protection of all the Council's information assets against loss, misuse or abuse.
- Make all users aware of the relevant UK and European Community legislation, and their responsibilities.
- Create an awareness that appropriate security measures must be implemented across the Council as part of the effective operation and support of Information Security.
- Make all users understand their own responsibilities for protecting the confidentiality, integrity and availability of the data they handle.

This Policy should be read in conjunction with the Council's Data Protection Policy which provides more detailed guidance on protecting personal data and satisfy the GDPR requirement for a formal statement of the Council's security arrangements for personal data.

2. SCOPE

All Council staff and councillors who may have access to information held by or on behalf of the Council, must adhere to the Council's Information Security Policy. The scope of the policy covers their use of Council-owned/leased/rented and on-loan facilities.

The policy applies throughout the lifecycle of the information from creation, storage, and use to disposal. It applies to all information including:

- Information stored electronically on databases or files and/or processed by applications, e.g. email.
- Information stored on computers, PDAs, mobile phones, printers, or removable media such as hard disks, CD rom, memory sticks, tapes and other similar media.
- Information transmitted on networks.
- Information sent by fax or other communications methods.
- All paper records.
- Microfiche, visual and photographic materials including slides and CCTV.
- Spoken, including face-to-face, voicemail and recorded conversation.

Although the use of social media resources by Council staff and Councillors is unrestricted and not centrally moderated, the Council requires its staff and Councillors to ensure they respect this policy and cause no damage to the Council's reputation.

3. RESPONSIBILITIES

All Council staff, councillors and authorised third parties must adhere to the Council's Information Security Policy. Compliance with the policy forms part of the Terms and Conditions of Service for Council staff and is implied via the Councillors Code of conduct.

4. COMPLIANCE WITH LEGISLATION

The Council has an obligation to abide by all UK legislation.

The requirement for compliance devolves to all users, who may be held personally responsible for any breach of the legislation.

5. MONITORING ELECTRONIC COMMUNICATIONS

The Council will exercise its right to intercept and monitor electronic communications received by and sent from the Council for the purposes permitted under legislation. The purposes cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to the system, e.g. hacking and denial of service attacks, ensuring the effectiveness of its operations and compliance with Council policies and regulations.

6. INFORMATION SECURITY INCIDENTS

Anyone suspecting that there has been, or is likely to be an information security incident, such as a breach of confidentiality, availability, integrity of information, or misuse of an information asset, should inform the Clerk immediately.

In the event of a suspected or actual information security incident or an unacceptable network event, the Clerk will report to the Council and carry out any necessary investigations.

7. SECURITY EDUCATION AND TRAINING

Council staff, Councillors and approved third parties, should be instructed on the Council's policy relating to information security and given training on the procedures relating to the security requirements of the work they are to undertake and on the correct use of the Council's IT assets in general before access to IT services is granted. They should be made aware of this policy including the reporting procedures in section 6.

8. SECURITY CONSIDERATIONS FOR EMPLOYMENT

Security roles and responsibilities, as laid down in this Policy should be included in job descriptions, where appropriate. These should include any general responsibilities for implementing the security policy as well as any specific responsibilities for the protection of assets, or for the execution of security processes or activities.

9. PROTECTING SENSITIVE DATA

It's essential that the Council protects sensitive data with enhanced security measures. Sensitive data can be defined as any information which is:

- Commercially sensitive administrative / planning data
- Commercially sensitive research data, and data which could bring harm if exposed to third parties
- Personal and Sensitive Personal data as defined under GDPR

Sensitive data must not be stored on or communicated through services which are not provided by the Council such as personal email or web-based 'cloud' storage services.

For guidance on protecting sensitive personal data, refer to Council's Data Protection Policy.

Databases and computers containing sensitive data must be protected with security controls. These must be password protected so that unauthorised access to data is restricted. Where possible, data should be anonymised to remove personal identifiers. Computers containing sensitive data must be disposed of properly to ensure all data has been wiped off properly.