SEALAND COMMUNITY COUNCIL

INFORMATION SECURITY POLICY - 2025

The purpose of the policy is to ensure the confidentiality, integrity and availability of information is maintained by implementing best practices to minimise risk. This policy provides practical guidance for staff, Councillors, and any contractors to ensure that information is handled securely in all forms.

Information exists in many forms. Information stored electronically, including in cloud-based systems or accessed remotely, must be secured using council-approved methods and access controls, including -

- Printed or written on paper
- Stored electronically
- Published on the internet
- Transmitted by post or electronically
- Conversational and voice recorded

Information Security requires the adherence to both the Record Management and the Data Protection polices of the Council.

All data must be processed in accordance with the UK GDPR and the Data Protection Act 2018.

Roles and Responsibilities

Information Security is primarily vested in the staff employed by the Council. However, individual councillors are also required to meet the objectives of these policies as well as those contained within the Standing Orders and Code of Conduct.

Where sensitive information is provided, all recipients are expected to respect the nature of such information and afford it the appropriate level of security. Such security will include the prevention of access by unauthorised personnel.

Clerk/RFO: Responsible for overall compliance with this policy, monitoring security practices, and reporting any breaches or incidents.

Councillors: Expected to comply with this policy, and report any potential breaches or security risks when using emails and devices for official business.

Contractors: Must follow the Council's security standards.

Cybersecurity Measures

- Devices must have antivirus protection, firewalls, and regular security updates installed.
- Councillors, staff and contractors must be vigilant against phishing, ransomware, and other cyber threats.
- Electronic data should be encrypted where possible.
- Personal devices should only be used for Council business unless the above is adhered to.

All staff and Councillors must immediately report any actual or suspected data breaches or security incidents to the Clerk.

Training and Awareness

Councillors and staff will receive periodic guidance and training on data protection, record management, and cyber threats.

Updates on practical security reminders will be provided at Council meetings or via official communications.

Nothing within this policy, or those for Record Management and Data Protection, will detract from the basic principles of the Freedom of Information Act.

This Policy was reviewed and agreed by Council at its meeting held on 20th October 2025

This policy will be reviewed periodically or sooner if there are changes in legislation or technology.

A Griffiths - Clerk and Responsible Financial Officer

October 2025