

SEALAND COMMUNITY COUNCIL

INFORMATION SECURITY POLICY

This policy ensures the confidentiality, integrity, and availability of information by implementing appropriate and proportionate security measures to minimise risk.

This policy provides practical guidance for Councillors, the Clerk/RFO, staff, and contractors to ensure information is handled securely in all forms.

Information exists in many forms, including:

- Printed or written on paper;
- Stored electronically, including in cloud-based systems;
- Published on the internet;
- Transmitted by post or electronically; and
- Conversational or voice-recorded.

Information security requires adherence to the Council's Records Management and Data Protection Policies.

All personal data must be processed in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended, and the Data (Use and Access) Act 2025.

Roles and Responsibilities

The Council, its Councillors, the Clerk/RFO, and any contractors or service providers handling Council information are responsible for information security.

Clerk/RFO

The Clerk/RFO is responsible for overall compliance with this policy, monitoring security practices and ensuring that actual or suspected security incidents and personal data breaches are appropriately dealt with and recorded.

Where a personal data breach must be reported to the Information Commissioner's Office (ICO), the Clerk/RFO will ensure the appropriate statutory requirements and timescales are followed.

Councillors

Councillors are expected to comply with this policy and the Council's related policies, Standing Orders and Code of Conduct.

Councillors must take reasonable steps to protect Council information when using email, computers, mobile devices or other systems for official Council business. They must report any actual or suspected security incident or data breach to the Clerk/RFO without undue delay.

Contractors

Contractors and service providers must follow the Council's appropriate security requirements when handling Council information.

Where a contractor processes personal data on behalf of the Council, the Council will maintain appropriate contractual and security arrangements in accordance with applicable data protection legislation.

Information Security

Where sensitive or confidential information is provided, all recipients are expected to respect the nature of such information and afford it an appropriate level of security.

Such security will include preventing access by unauthorised persons and appropriately protecting information against loss, alteration, destruction, or unauthorised disclosure.

Access to Council information should be limited to those who are authorised and require access for legitimate Council purposes.

Cybersecurity Measures

The Council will take appropriate and proportionate measures to protect its information and systems from cyber threats.

These measures include, where appropriate:

- Devices should have suitable antivirus/anti-malware protection, firewalls and current security updates;
- Councillors, staff and contractors must remain vigilant against phishing, ransomware, malware and other cyber threats;
- Electronic data should be encrypted where appropriate to the level of risk;
- Appropriate passwords and authentication controls should be used;
- Multi-factor authentication should be used where available and appropriate;
- Council information should be appropriately backed up where necessary; and
- Personal devices should only be used for Council business where appropriate security measures are in place.

All staff and Councillors must report any actual or suspected data breach or information-security incident to the Clerk/RFO without undue delay.

Personal Devices

Where personal devices are permitted for Council business, staff must maintain reasonable security measures, including appropriate passwords or authentication, current security updates, and protection against unauthorised access.

Council information should not be retained on personal devices for longer than reasonably necessary and should be securely removed when no longer required.

Data Breaches

The Council will assess actual or suspected personal data breaches and take appropriate action to contain, investigate, record and, where legally required, report the breach.

Where notification to the ICO is required, the Council will comply with applicable statutory requirements, including notifying the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Personal data breaches will be recorded appropriately, including where notification to the ICO is not required.

Training and Awareness

Councillors and staff will receive appropriate guidance and training on data protection, records management, information security and cyber threats.

Updates on practical security matters may be provided at Council meetings or through official Council communications.

Freedom of Information

Nothing within this policy, or the Council's Records Management and Data Protection Policies, will detract from the Council's statutory obligations under the Freedom of Information Act 2000 or other applicable information-access legislation.

Information-security and confidentiality considerations will be taken into account when handling information requests, but will not be used to prevent disclosure where disclosure is legally required.

Review of Policy

This policy will be reviewed at least annually, or sooner where there are changes in legislation, regulatory requirements, relevant guidance, Council systems, technology or working practices that may materially affect information security.

Read this policy in conjunction with the Council's Records Management Policy, Data Protection Policy, Standing Orders, and Code of Conduct.

This policy was reviewed and approved by Sealand Community Council at its meeting held on: 21st September 2026.

A Griffiths – Clerk of the Council – September 2026