Redgrave Parish Council

INFORMATION SECURITY INCIDENT POLICY

Policy Statement

Redgrave Parish Council (RPC) is committed to maintaining the highest standards of information security and data protection. This policy ensures that information security incidents are identified, reported, and managed effectively in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, SAPPP 2025 (Proper Practices), and NALC model policies (2023–2024).

The policy forms part of RPC's governance and risk management framework and contributes to compliance with the Annual Governance and Accountability Return (AGAR) Section 1, Assertion 5 (Risk Management and Data Protection).

Purpose and Scope

This policy provides a framework for identifying, reporting, and responding to information security incidents that may affect the confidentiality, integrity, or availability of RPC information. It applies to all councillors, committees, staff, contractors, and volunteers who handle information on behalf of Redgrave Parish Council.

Definition of an Information Security Incident

An information security incident is any event that could compromise the security, confidentiality, integrity, or availability of RPC information systems or data. Examples include (but are not limited to):

- The loss or theft of equipment or data.
- Unauthorised access to personal or confidential information.
- Accidental disclosure of personal data.
- Malware infection or system compromise.
- Human error leading to data exposure.
- Failure of third-party service providers handling Council data.

Reporting an Incident

All suspected or actual information security incidents must be reported immediately to the Parish Clerk. If the incident involves the Clerk, the matter should be reported to the RPC Chair.

Reports should include details of the incident, the data or systems affected, and any actions already taken. The Clerk will maintain a confidential incident log and initiate appropriate investigation and response steps.

The Clerk will require reporting individuals to supply the following information:

- Contact name and number of persons reporting the incident.
- The type of data or information involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

Investigation and Response

The Parish Clerk will assess the nature and impact of the incident within 24 hours of receiving the report. The Parish Clerk will then undertake the following actions:

- Contain the incident and prevent further loss or damage.
- Assess the scale and type of information affected.
- Determine if personal data has been compromised.
- Notify the Chair.
- Implement remedial measures and record all actions taken.

GDPR and Data Breach Reporting

In accordance with Article 33 of the UK GDPR, if a personal data breach is likely to result in a risk to individuals' rights or freedoms, the Parish Clerk must notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

Where a breach poses an elevated risk to affected individuals, those individuals will also be informed without undue delay, providing advice on steps they can take to protect themselves.

Any third-party processor acting on behalf of RPC must notify the Parish Clerk without undue delay if they become aware of a personal data breach.

Confidentiality and Record Keeping

All information relating to an information security incident will be treated as confidential and processed lawfully under Article 6(1)(e) UK GDPR (performance of a public task). Incident records will be retained securely in accordance with the RPC's Document Control and Records Management Policy for audit and governance purposes.

Incident records will include the date, nature, impact, and resolution of each event and will be available for inspection by the internal auditor as part of the RPC's SAPPP 2025 compliance framework.

Freedom of Information and Transparency

Information relating to individual incidents is exempt from disclosure under the Freedom of Information Act 2000 (Sections 31 and 40). However, RPC may publish anonymised summaries of incidents and corrective actions taken to demonstrate accountability.

This policy will be published on the RPC's website in accordance with the Local Government Transparency Code 2015.

Responsibilities

The Parish Clerk is responsible for managing this policy, maintaining the incident log, and ensuring prompt response to security events.

The Chair may oversee investigations where appropriate.

All councillors, staff, and contractors are responsible for promptly reporting suspected incidents and cooperating with investigations.

Data processors must have written agreements with the RPC that include incident notification requirements.

Examples of Information Security / Misuse Incident Protocols

Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

Malicious Incident

- Computer infected by a virus or other malware (for example spyware or adware).
- An unauthorised person changing data.
- Receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Social engineering - Unknown people asking for information which could gain them access to council data (e.g., a password or details of a third party).
- Unauthorised disclosure of information electronically, in paper form or verbally.
- Falsification of records, Inappropriate destruction of records.
- Damage or interruption to Council equipment or services caused deliberately e.g., computer vandalism.
- Unauthorised Information access or use.
- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Printing or copying confidential information and not storing it correctly or confidentially.

Access Violation

- Disclosure of logins to unauthorised people.
- Disclosure of passwords to unauthorised people e.g., writing down your password and leaving it on display.
- Accessing systems using someone else's authorisation e.g., someone else's user ID and password.
- Inappropriately sharing security devices such as access tokens
    - Other compromise of user identity e.g., access to network or specific system by unauthorised person .

Environmental

- Loss of integrity of the data within systems and transferred between systems.
- Damage caused by natural disasters e.g., fire, burst pipes, lighting etc.
- Deterioration of paper records.
- Deterioration of backup tapes.
- Introduction of unauthorised or untested software.
    - Information leakage due to software errors.

Inappropriate use

- Accessing inappropriate material on the internet.
- Sending inappropriate emails.
- Personal use of services and equipment in work time.
- Using unlicensed Software.
- Misuse of facilities, e.g., phoning premium line numbers.

Theft / loss Incident

- Theft / loss of data – written or electronically held.
- Theft / loss of Council equipment including computers, monitors, mobile phones, smart phones, memory sticks, CD or other storage devices.

Accidental Incident

- Sending an email containing sensitive information to 'all staff' by mistake.
- Receiving unsolicited mail of an offensive nature, e.g., containing pornographic, obscene, racist, sexist, grossly offensive or violent material.
- Receiving unsolicited mail which requires you to enter personal data.

Mis-keying

- Receiving unauthorised information.
- Sending information to wrong recipient.

Escalation

The Clerk will contact the Suffolk Association of Local Councils for advice on any valid security incident where appropriate.

SALC
Unit 11a, Hill View Business Park
Old Ipswich Road
Claydon
Ipswich
IP6 0AJ
Tel: 01473 833713
E-Mail: admin@salc.org.uk

Review and Governance

This policy will be reviewed annually or sooner if legislation, SAPPP guidance, or best practice changes. Compliance with this policy will be confirmed as part of the Annual Governance and Accountability Return (AGAR) review process.