Barrowby Parish Council

Email: clerk@barrowbyparishcouncil.gov.uk
Address: Reading Room, Church Street, Barrowby, NG32 1BX
Website: https://barrowby.parish.lincolnshire.gov.uk

IT / Cyber Security Incident Report Procedure

Document control

- **Owner:** Full Council
- **Responsible officer:** Clerk / Proper Officer
- **Adopted:** 11.05.2026 (Minute ref: 8e [26/008])
- **Version:** 2025.1
- **Review:** Annually or earlier if legislation/guidance changes
- **Next review due:** January-March 2027 at Full Council for formal adoption at Parish Council May 2027

1. Purpose

This procedure sets out how Barrowby Parish Council will report, record, assess and respond to IT and cyber security incidents.

2. What must be reported

The following must be reported immediately to the Clerk / Proper Officer:

- lost or stolen devices used for Council business;
- suspicious or successful phishing emails;
- malware, ransomware or virus alerts;
- unauthorised access or suspected account compromise;
- emails sent to the wrong recipient;
- accidental deletion, disclosure or alteration of Council information;
- loss of paper or electronic records;
- any other event that may affect the confidentiality, integrity or availability of Council information or systems.

3. Immediate action by the user

The user must:

- report the incident immediately;
- stop and contain the issue where safe to do so, for example disconnecting from Wi-Fi or not opening further suspicious emails;
- not delete evidence unnecessarily;
- follow any instruction given by the Clerk / Proper Officer or IT support.

4. Logging and assessment

The Clerk / Proper Officer will:

- record the date, time, nature of incident and person reporting;
- assess the likely impact and urgency;
- decide whether IT support, the DPO, insurer or another authority should be contacted;
- determine whether the incident amounts to a personal data breach and requires escalation.

5. Containment and recovery

Appropriate steps will be taken to contain and recover from the incident, which may include:

- password resets;
- account suspension;
- device isolation;
- deletion or recall of misdirected emails where possible;
- restoration from backup;
- additional monitoring or security measures.

6. Review

Serious incidents, repeated incidents, or incidents revealing a weakness in controls will be reviewed and may lead to updated procedures, training or policy changes.

7. Record keeping

A written incident log will be maintained by the Council and retained in accordance with the Council's retention arrangements.