Trowell Parish Council IT Recovery Strategy

Adopted: 11 November 2025

1. Purpose and Scope

This IT Recovery Strategy sets out the procedures and responsibilities for restoring Parish Council IT systems and data following a disruption.
It covers:

- Parish Council computers, laptops, and mobile devices
- Cloud-based and locally stored data
- Email and communication systems
- Website and social media accounts
- Financial, governance, and statutory records

---

2. Objectives

- Minimise downtime and service disruption.
- Ensure rapid restoration of essential systems and data.
- Protect sensitive and statutory data.
- Maintain compliance with GDPR and data protection laws.
- Maintain transparency and communication with the community.

---

3. Risk Assessment

Common risks include:

Risk	Impact	Likelihood	Mitigation
Hardware failure	Medium	Medium	Regular backups, device replacement plan
Cyber attack / ransomware	High	Medium	Anti-virus, MFA, user training, secure backups
Accidental data deletion	Medium	Medium	Versioned cloud backups
Power outage	Low	Low	Use of laptops and cloud systems
Fire/flood/theft	High	Low	Off-site and cloud backups
Loss of key personnel	High	Low	Shared admin credentials stored securely

---

4. Backup Strategy

- **Frequency:** Daily automated backups of all Council data (documents, emails, finance systems).

- **Storage:**
  - **Primary:** Secure cloud service (e.g. Microsoft 365, Google Workspace).
  - **Secondary:** Weekly offline backup on encrypted external drive, held off-site.
- **Retention:** Keep backups for at least 90 days.
- **Testing:** Backup recovery tests every 6 months.

---

5. Recovery Procedures

Step 1: Assess the Situation

- Determine the cause and scope of the disruption.
- Record the incident in the Council's IT incident log.
- Notify the Clerk and Chair immediately.

Step 2: Initiate Recovery

- Activate backup restoration procedures.
- If local hardware is affected, use replacement devices or cloud access from alternative devices.
- Restore critical systems in order of priority:
  1. Email and communication systems
  2. Access to financial systems and statutory documents
  3. Website and public communications
  4. Secondary systems (archives, non-urgent files)

Step 3: Verification

- Confirm data integrity after restoration.
- Validate access permissions and passwords.
- Report recovery status to the Council.

Step 4: Review and Report

- Document what happened and lessons learned.
- Update procedures to prevent recurrence.
- Report any data breaches to the ICO if applicable (within 72 hours).

---

6. Roles and Responsibilities

Role	Responsibility
Parish Clerk	Oversees recovery process, communicates with members and public, maintains IT asset register.
Chair/Vice-Chair	Authorises recovery actions, ensures governance oversight.

Role	Responsibility
IT Support Provider	Technical restoration, backup management, and cyber security.
All Councillors/Staff	Follow data security policies, report incidents immediately.

---

7. Communication Plan

- Internal notification via personal email or phone.
- Public updates posted on website and noticeboards if disruption affects service delivery.
- Liaise with local authorities or NALC (National Association of Local Councils) if necessary.

---

8. Preventive Measures

- Maintain up-to-date antivirus and operating systems.
- Enforce strong passwords and MFA.
- Provide annual cybersecurity awareness training.
- Review IT suppliers and contracts annually.

---

9. Testing and Review

- Conduct annual IT recovery drill.
- Review and update this plan every 12 months or after a major incident.

---

10. Appendices

- **A:** IT Asset Register
- **B:** Backup Schedule
- **C:** Key Contacts (IT provider, Clerk, Chair, hosting provider, etc.)
- **D:** Incident Log Template