Dalton Town Council – Data Audit Policy & Annual Audit Guide

Linked Policy: Data Protection Policy
Responsible Officer: Town Clerk / Data Protection Officer (DPO)

---

1. Why We Do This

We audit our data to make sure the Council handles personal information safely and legally. Goals:

- Spot and fix data problems.
- Follow rules for keeping and deleting data.
- Make sure everyone does things the same way.
- Show residents, staff, and councillors we are responsible with data.

---

2. What Data This Covers

- Emails, council software, and other digital records.
- Paper records like meeting notes, forms, letters.
- Data shared with outside contractors or service providers.
- Information about residents, staff, councillors, and volunteers.

---

3. Who Does What

- **Town Clerk / DPO:** Plans and runs audits, keeps the data register, ensures rules are followed.
- **Staff & Councillors:** Help with audits, follow rules for keeping data, and act on recommendations.

---

4. How Often We Audit

- **Full Audit:** Check all data and processes — once a year.
- **Targeted Audit:** Focus on tricky or new areas — quarterly or as needed.
- **Retention Check:** Make sure data is kept and deleted according to rules — once a year.

- **Admin Checks:** Staff review emails and resident records every 3–6 months.

---

5. What We Check

1. **Data Mapping** – Make sure we know what data we have, why we have it, who owns it, and where it's stored.
2. **Security** – Check passwords, access rights, locked cabinets, backups, and who can see the data.
3. **Retention & Disposal** – Make sure old data is deleted safely and only kept as long as needed.
4. **Data Sharing / Third Parties** – Check contracts and agreements with anyone we share data with.
5. **Training & Awareness** – Make sure staff and councillors know their responsibilities.
6. **Record Findings** – Note what's okay, what's wrong, and what needs fixing.

---

6. Reporting & Actions

- Write a simple report showing findings and risks.
- Submit to the Council or committee.
- Assign actions with deadlines.
- Feed results into the Council's risk management system.

---

7. Sign-Off (Simplified for Dalton Town Council)

Who signs and when:

1. **Auditor (AGAR / annual check)** – signs in **April**, after checking financial and related records. Confirms the audit is done properly.
2. **Town Clerk / DPO** – confirms that:
    - all issues from the auditor or staff checks are noted, and
    - actions are assigned and tracked for completion.

Ongoing Checks:

- Admin staff check emails, resident records, and other documents **every 3–6 months**.
- Any issues are reported to the Town Clerk / DPO.

Checklist Version:

- Auditor has reviewed records for the AGAR (April).
- Admin staff have checked emails and records (3–6 monthly).
- Town Clerk / DPO has noted all findings.
- Actions assigned to the right staff.
- Follow-up dates set and tracked.

---

8. Yearly Audit Plan (Simplified)

Audit Type	Frequency	Responsible	Notes / Output
Full Data Audit	Annually	Town Clerk / DPO	Comprehensive review of all data, retention, and security. Report findings to Council.
Financial Audit (AGAR)	Annually (April)	Auditor / Town Clerk / DPO	Auditor checks all records and signs AGAR. Town Clerk / DPO tracks any issues.
Targeted Audit	Quarterly or as needed	Town Clerk / DPO	Focus on new systems, high-risk areas, or sensitive data. Recommendations for improvements.
Retention & Disposal Check	Annually	Town Clerk / DPO	Verify data is kept or deleted according to the retention schedule.
Admin Staff Checks	Every 3–6 months	Admin Staff	Spot-check emails, resident records, and other routine data. Report issues to Town Clerk / DPO.
Training & Awareness Review	Annually (or as needed)	Town Clerk / DPO	Ensure staff and councillors are trained in GDPR and data handling. Schedule refreshers if required.

Audit Type	Frequency	Responsible	Notes / Output
Data Sharing / Third Parties Review	Annually (or as needed)	Town Clerk / DPO	Check contracts, agreements, and DPIAs. Ensure compliance with GDPR.
Risk Review	Mid-year & Year-end	Town Clerk / DPO	Update risk register with audit findings, assign actions, track progress.

---

9. Keeping It Current

- Review this policy every year or if data systems/rules change.
- Any changes must be approved by Council and shared with staff.

Quick Audit Checklist (Plain Version)

Audit Type: Full / Targeted / Retention

1. Data Mapping

- Check we know what data we have, why, who owns it, where it's stored.
- Examples: Residents' contact info, staff records, councillor info, meeting minutes, complaints.

2. Security

- Check digital passwords, shared drives, email access.
- Check paper records are locked.
- Check backups exist.

3. Retention & Disposal

- Make sure old data is deleted safely.
- Examples: Staff files after 6 years, invoices after 7 years, complaints after 3 years.

4. Data Sharing / Third Parties

- Check agreements exist.
- Make sure contractors follow GDPR rules.

5. Training & Awareness

- Check staff, councillors, volunteers know their responsibilities.
- Schedule refresher training if needed.

6. Findings & Actions

- Note any problems.
- List actions, assign people, and set deadlines.