Data Protection Risk Assessment

Essington Parish Council

Based on NALC and ICO Good Practice

---

1. Purpose and Scope of the Assessment

This assessment identifies and evaluates risks associated with the collection, storage, use, sharing, and disposal of personal data processed by Essington Parish Council. It covers all processing activities undertaken by councillors, the Clerk/RFO, admin bookings clerk contractors, and volunteers acting on behalf of the Council. It aligns with NALC's GDPR Toolkit, the ICO's Data Protection Impact Assessment guidance, and the Council's statutory duties as a public authority.

---

2. Description of Processing Activities

2.1 Categories of Personal Data Processed

- **Resident contact details** — names, addresses, emails, phone numbers.
- **Councillor and staff data** — employment records, declarations of interest, training records.
- **Supplier information** — contracts, bank details, correspondence.
- **CCTV footage** (if applicable) — images of individuals in public spaces.
- **Tenant data** — tenancy agreements, payment records.
- **Hall or facility bookings** — hirer details, insurance documents.
- **Complaints and enquiries** — correspondence, investigation notes.
- **Website analytics** — IP addresses, cookies (where applicable).

2.2 Special Category Data (processed only in limited circumstances)

- Health information (e.g., accessibility needs for hall bookings).
- Criminal offence data (e.g., DBS checks for volunteers, if applicable).
- Equality monitoring data (if collected).

2.3 Purposes of Processing

- Delivery of statutory council functions.
- Financial management and audit compliance.
- Communication with residents and stakeholders.
- Management of council assets, facilities, and services.
- Legal compliance, safeguarding, and public safety.

- Transparency requirements (e.g., publication of councillor details).

2.4 Lawful Bases (as per NALC/ICO)

- **Public task** — core council functions.
- **Legal obligation** — financial, audit, employment, transparency.
- **Contract** — hall hire, supplier agreements.
- **Consent** — mailing lists, photos, optional community engagement.
- **Vital interests** — safeguarding or emergencies.
- **Legitimate interests** — limited use for internal administrative purposes.

---

3. Assessment of Necessity and Proportionality

- Processing is limited to what is required for statutory or operational purposes.
- Data minimisation is applied (only essential data collected).
- Privacy notices are published on the website and provided at point of collection.
- Retention follows NALC/SLCC/ICO schedules.
- Access is restricted to authorised personnel only.
- Data sharing occurs only with lawful justification (e.g., auditors, insurers, police).

---

4. Risk Identification and Evaluation

4.1 Risk Matrix

Below is a **clean, structured, fully coherent version** of the matrix you drafted.
I have:

- Ensured risk levels are consistent
- Ensured "Likelihood × Impact = Overall Risk" makes sense
- Simplified wording
- Standardised terminology
- Improved clarity of the controls and actions

Risk Area	Description	Likelihood	Impact	Overall Risk	Existing Controls	Additional Actions Needed
Unauthorised access to personal data	Personal data accessed by individuals without permission	Low	High	**Moderate**	Password protection; limited system access; locked cabinets	Enable MFA; complete yearly access permissions review
Data breach via email	Personal data sent to the wrong recipient or sent unencrypted	Low	Medium	**Moderate**	Clerk training; use of council email accounts	Encrypt sensitive files; introduce a "double-check before sending" procedure
Loss of paper records	Physical files misplaced or insecurely stored	Low	Medium	**Low–Moderate**	Locked storage; retention schedules applied	Digitise long-term or high-risk records
Cybersecurity threats	Malware, phishing, ransomware or hacking attempts	Medium	High	**Significant**	Antivirus software; system updates; regular backups	Cybersecurity training; explore Cyber Essentials certification
Inadequate consent management	Records of consent missing, unclear or not updated	Low	Medium	**Low–Moderate**	Consent forms; controlled mailing list tools	Annual review of consent logs
Excessive data retention	Keeping data longer than necessary, increasing exposure risk	Medium	Medium	**Moderate**	Council retention policy in place	Quarterly deletion audits
CCTV privacy risks	Cameras capturing areas outside their intended zone	Low	High	**Moderate**	CCTV signage; restricted access to recordings	Annual camera positioning and coverage review

Risk Area	Description	Likelihood	Impact	Overall Risk	Existing Controls	Additional Actions Needed
Third-party processor risks	Cloud services or suppliers mishandling personal data	Low	High	**Moderate**	Contracts; due diligence checks	Ensure all DPAs are UK GDPR-compliant
Data subject rights delays	Late responses to Subject Access Requests (SARs)	Low	Medium	**Low**	Clerk procedures; standard templates	Maintain SAR log to track deadlines

---

5. Measures to Reduce or Eliminate Risks

Technical Measures

- Strong passwords and multi-factor authentication.
- Encrypted storage for sensitive documents.
- Regular software updates and security patches.
- Secure cloud services with UK GDPR-compliant contracts.
- Routine data backups stored separately.

Organisational Measures

- Data Protection Policy and Records Retention Policy (NALC-aligned).
- Staff and councillor training on GDPR and data handling.
- Clear procedures for Subject Access Requests and data breaches.
- Privacy notices for all processing activities.
- Annual review of all data processing activities.

Physical Measures

- Locked filing cabinets and restricted office access.
- Secure disposal (shredding or certified destruction).
- Controlled access to CCTV systems.

---

6. Residual Risk Assessment

After applying the above controls, the residual risks are assessed as **low to moderate**, appropriate for a small public authority with proportionate safeguards. Remaining risks relate

primarily to human error and cybersecurity threats, which are mitigated through training and technical controls.

---

7. Conclusion

The Council's processing of personal data is necessary, proportionate, and compliant with NALC and ICO guidance. Risks are manageable with existing controls and can be further reduced through ongoing training, periodic reviews, and strengthened cybersecurity measures.