

Reviewed and approved:

Next review date:

GDPR Data Map and Risk Assessment - Durrington Town Council

Purpose of Processing	Categories of Personal Data	Recipients (Data Sharing)	Processors	Article 6 Lawful Basis	Article 9 Condition	Storage and Security	Anonymisation / Minimisation	Risk Level & DPIA
Minutes and Agendas	Contact information, identity	None	Website and email provider; cloud storage provider	Legal obligation	N/A	Signed hard copies stored in Council office. Unsigned electronic copies are held on Clerk's password-protected laptop and shared with councillors. Councillors may hold copies on personal devices.	No identifying information about private individuals included. Employee data anonymised or withheld where possible.	Low risk. DPIA not required.
Accounts, Grants, Tenders, Invoices and Payments	Contact information, identity, bank details	Internal and external auditors; Bank	Cloud storage provider; website and email provider; Scribe	Legal obligation; Contract	N/A	Clerk holds hard and electronic copies securely. Limited copies held by councillors for authorised payment processing.	Data is shared only with councillors involved in financial processing.	Low risk. DPIA not required.
General Correspondence and Administration	Contact information, identity; special category data where provided	Other Parish, Town, or County/Unitary Councils; competent authorities	Cloud storage and email provider; Office 365	Public task; Legal obligation; Contract	Consent where applicable	Stored securely by Clerk in hard copy and electronic form. Councillors may hold copies where necessary.	Consent obtained where required. Data anonymised if consent is not obtained. BCC used for group emails.	Low risk. DPIA not required.
Payroll and Pensions	Contact information, identity, bank details	HMRC; LGPS	Cloud storage and email provider; Payroll software	Legal obligation	N/A	Records held securely by Clerk on dedicated password-protected device.	Shared only for authorised payroll and payment purposes.	Low risk. DPIA not required.

Purpose of Processing	Categories of Personal Data	Recipients (Data Sharing)	Processors	Article 6 Lawful Basis	Article 9 Condition	Storage and Security	Anonymisation / Minimisation	Risk Level & DPIA
HR Records	Contact information, identity, bank details; special category data	None	Cloud storage and email provider	Contract	Employment, social security, and social protection	Stored securely by Clerk with restricted access.	Shared only where necessary. Data anonymised where possible.	Medium risk. DPIA not required at present.
Councillor Information	Contact information, identity; special category data	Monitoring Officer; competent authorities,	Website and email provider; cloud storage provider	Legal obligation	Substantial public interest	Electronic and hard copy records stored securely, including locked filing cabinet.	Shared only where required and anonymised where appropriate.	Low risk. DPIA not required.
Complaints, Code of Conduct, and Investigations	Contact information, identity; special category data	Monitoring Officer; competent authorities	Cloud storage and email provider	Legal obligation; Public task	Substantial public interest	Stored securely by Clerk with restricted access.	Shared on a strict need-to-know basis and anonymised where possible.	Medium risk. DPIA considered case by case.
FOI, EIR, and Subject Access Requests	Contact information, identity	Requesting individual; ICO where required	Cloud storage and email provider	Legal obligation	N/A	Requests and responses stored securely with access controls.	Personal data redacted prior to disclosure where required.	Low risk. DPIA not required.
CCTV	Images of individuals	Police or authorised authorities	None	Public task	Substantial public interest	Footage stored for 28 days on secure recorder. Incident footage stored on USB in office safe.	Footage overwritten after 28 days unless required for an incident.	Medium risk. DPIA completed.

To be read with the following policies:

Data Protection Policy
 Privacy Notice
 Retention Schedule
 IT / Information Security Policy
 Data Breach Policy and CCTV Policy

Council members to be made aware of their responsibilities by:

Relevant Policies
 Training
 Regular reminders
 Dedicated email addresses