

GDPR Risk Assessment

This document enables Duloe Parish Council to identify the risks it faces and to confirm that appropriate measures are in place to reduce them. In carrying out this assessment, the Council followed the plan outlined below.

- Identify the areas requiring review.
- Determine the potential risks.
- Assess how each risk is managed and controlled, and record all findings.
- Review, evaluate, and update the assessment as necessary.

Subject	Risk(s) Identified	H/M/L	Management/Control of Risk	Review/Assess/Revise
All personal data	Personal data accessed by unauthorised third parties	H	Identify all personal data held (e.g., Electoral Roll, applications, tenancy agreements), the purpose, retention period, and any data-sharing arrangements.	Conduct Data Audit
	Personal data published in minutes or council documents	M	Identify all stored personal data across paper and electronic systems, including portable devices.	Delete emails older than 6 months if no longer required

Sharing of data	Personal data shared inappropriately	L	Confirm any data-sharing with other organisations and establish written agreements where required.	Share only with organisations with equivalent data-protection standards
Hard copy data	Hard copy data accessed by unauthorised persons	L	Retain only necessary data; destroy data in line with the Retention Policy; store sensitive data securely.	Destroy confidential waste routinely; procedure adequate
Electronic data	Theft or loss of devices containing personal data	L	Ensure all devices are password-protected.	Procedure adequate
	Loss or theft of devices used for council emails	M	Remind councillors to protect devices and handle council emails securely.	Reinforced through this document
	Loss of data due to insufficient backups	H	Carry out regular data backups.	Monthly
	Unsafe disposal of IT equipment	L	Securely wipe or destroy devices before disposal.	Procedure adequate
Email security	Unauthorised access to council emails	H	Maintain up-to-date antivirus software and firewalls.	Procedure adequate
	Inappropriate access to email accounts	L	Use dedicated council email addresses for staff and councillors.	Complete
	Accidental disclosure via group emails	L	Use BCC for group emails.	Procedure adequate

	Exposure of IP addresses	M	Copy content into a new email before sending externally.	Procedure adequate
	Forwarding personal information unnecessarily	L	Do not forward emails from the public; copy essential information into a new email with personal data removed.	Procedure adequate
	Retention of unnecessary emails	L	Delete emails once queries are resolved.	After 6 months
General internet security	Unauthorised access to council computers or files	M	Password-protect all devices; do not share passwords.	Procedure adequate
	Malware or hacking	H	Maintain up-to-date antivirus, firewalls, and encryption.	Procedure adequate
	Outdated operating systems	M	Install system updates regularly.	Procedure adequate
	Unauthorised access via shared drives	L	Password-protect sensitive folders; restrict shared-drive access.	Rarely an issue
Website security	Publishing personal information or images without consent	L	Obtain written consent (including parental consent for under-18s); consider need for a Vetting and Barring Policy.	Rarely an issue; explore policy requirement
Disposal of computers and printers	Data recovered from disposed equipment	L	Wipe or destroy hard drives before disposal.	Not yet required
Financial risks	Financial loss due to data-breach fines	L	Ensure adequate budget provision for GDPR compliance and security measures.	Procedure adequate

	Insufficient GDPR/Data Protection budget	H	Allocate sufficient funds for compliance and security.	To be considered
General risks	Loss of third-party data due to lack of awareness	L	Provide training to staff and councillors.	Ongoing
	Recording during confidential sessions	L	Ensure no recording devices remain in the room during closed sessions.	Rarely an issue

Adopted at the meeting held on 19th February 2026

Review of Risk Assessment due: Jan 2027