

General Data Protection Regulation (GDPR) Policy

Purpose of the Policy and Background to GDPR

This policy explains to councillors, staff, volunteers, and members of the public how Duloe Parish Council complies with the General Data Protection Regulation (GDPR).

Personal data must be:

- processed lawfully, fairly, and transparently
- collected for specified, explicit, and legitimate purposes
- adequate, relevant, and limited to what is necessary
- accurate and kept up to date
- retained only for as long as necessary
- processed securely

This policy updates all previous data protection policies to reflect the requirements of GDPR, which has applied in the UK since May 2018.

The Government has confirmed that GDPR remains a legal requirement following the UK's departure from the EU.

This policy sets out the duties and responsibilities of Duloe Parish Council and the measures the Council will take to meet its obligations.

2 Identifying Roles and Minimising Risk

GDPR requires that all members of the Council understand their responsibilities and that roles are clearly defined.

The Council is the Data Controller.

The Clerk/RFO is appointed as the Council's Data Protection Officer (DPO).

The DPO is responsible for:

- conducting an information audit
- managing the information collected by the Council
- issuing privacy notices
- responding to data requests and complaints
- ensuring the safe disposal of information

These responsibilities will be included in the Clerk/RFO/DPO's Job Description.

The appointment of the Clerk as DPO must avoid any conflict of interest; the DPO must not determine the purposes or manner of processing personal data.

All councillors and staff must take care when handling personal information, whether in hard copy or electronic form.

A breach of GDPR may result in fines from the Information Commissioner's Office (ICO) and compensation claims from affected individuals.

Handling personal data is considered a **medium risk** to the Council and must be included in the Council's Risk Management Policy.

Risks can be minimised through:

- regular information audits
- issuing privacy notices
- maintaining privacy impact assessments for new projects
- limiting who holds personal data
- ensuring councillors and staff receive data protection training

3 Data Breaches

The DPO is responsible for investigating all personal data breaches.

Any suspected breach must be reported to the DPO immediately.

Investigations must be completed within one month of the breach being reported.

Procedures are in place to detect, report, and investigate personal data breaches.

The ICO must be notified within **three days** if a breach is likely to pose a risk to individuals' rights and freedoms, including risks such as:

- discrimination
- reputational damage
- financial loss
- loss of confidentiality
- significant social or economic disadvantage

Where a breach poses a **high risk**, the DPO must also notify affected individuals directly.

It is unacceptable for unauthorised users to access IT systems using another person's login details or to use equipment while someone else is logged in.

Employees, volunteers, and councillors must not use IT systems in ways that could harm the Council, including discussing internal Council matters on social media.

4 Privacy Notices

Transparency is a key requirement of GDPR. Individuals must be informed about how their personal data is used.

A privacy notice explains what personal information the Council collects, why it is collected, how long it will be kept, and who to contact.

A privacy notice must include:

- the name and contact details of the Data Controller
- the name and contact details of the DPO
- the purpose of processing

- the retention period
- the individual's right to withdraw consent

Issuing a privacy notice must be recorded in the Council's Information Audit.

The Council will adopt a standard privacy notice, with adjustments made where necessary—for example, when processing children's data.

All privacy notices must be clear, accessible, and verifiable.

5 Information Audit

The DPO must maintain an information audit detailing:

- what personal data the Council holds
- where it came from
- why it is held
- who it is shared with

The audit must include both electronic and hard-copy information.

As Council activities change, the information held may also change.

The information audit will be reviewed at least annually or when new activities are undertaken.

The audit review should take place before the annual review of this policy and must be minuted.

6 Individuals' Rights

GDPR provides individuals with the following rights:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making, including profiling

GDPR strengthens two rights in particular:

- **Right to erasure** ("right to be forgotten") where data is no longer needed for its original purpose
- **Right to data portability**, which must be provided free of charge

Requests for deletion of information must be responded to within one month.

The DPO has delegated authority to delete information where appropriate.

If a request is manifestly unfounded, it may be refused or a charge may be applied, in line with the Council's Freedom of Information Publication Scheme. Duloe Parish Council will be informed of all such requests.

7 Children

Children's personal data is subject to special protection.

Children aged **13 or over** may give their own consent. For children under 13, consent must be obtained from a parent or guardian.

Consent forms for young people aged 13+ must be written in clear, age-appropriate language.

8 Summary of Required Actions

The Council must be registered with the ICO.

This policy will be published on Duloe Parish Council's website and treated as a core policy.

The Clerk's Contract and Job Description will be updated to reflect GDPR responsibilities.

An information audit will be conducted and reviewed at least annually or when services or projects change.

Privacy notices must be issued where required.

Data protection must be included in the Council's Risk Management Policy.

Duloe Parish Council will oversee and manage GDPR compliance.

9 Policy Review

This policy is based on current guidance and will be reviewed at least annually or when new advice is issued by the ICO.

All employees, volunteers, and councillors must comply with this policy at all times to protect privacy, confidentiality, and the interests of Duloe Parish Council.

Adopted at the meeting held on 19th February 2026

This policy to be next reviewed in April 2027