

Data Breach Policy

This Data Breach Policy is provided by Glapwell Parish Council.

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Notifying the Information Commissioners Office (ICO)

Currently, data breaches do not have to be routinely notified to the ICO or others although the ICO recommends that it is good practice so to do. However, guidance states that organisations should notify the Information Commissioners Office of a breach where it is likely to result in a risk to the rights and freedoms of individuals or if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Data Breaches will be recorded using the ICO's online system: <https://ico.org.uk/fororganisations/report-a-breach/> and the following information should be provided:

- a description of the nature of the personal data breach including, where possible:
 - a. the categories and approximate number of individuals concerned; and
 - b. the categories and approximate number of personal data records concerned
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Notifying the Individual concerned

If a breach is likely to result in a high risk to the rights and freedoms of individuals (such as through identity theft) the council will notify those concerned directly and without undue delay.

Timescales

Under the UK GDPR (as amended by the Data (Use and Access) Act), the Council must report a notifiable personal data breach without undue delay, and not later than 72 hours after becoming aware of it. If the notification takes longer than 72 hours, a robust written justification for the delay must be provided to the Information Commission. Information can be provided to the regulator in phases as an investigation unfolds, but the initial 72-hour filing deadline remains strict

Notifying the council

If anyone (including a third party) suspects that a data breach has occurred, details of the alleged breach must be reported **immediately** via the fastest available means (**telephone or email**) to ensure the Council can meet its statutory 72-hour reporting window. Councillors and staff must not wait to gather full evidence before alerting the Data Protection Officer:

Mrs D Greatorex, Data Protection Officer, Glapwell Parish Council, C/O The Glapwell Centre, The Green, Glapwell, Chesterfield, Derbyshire, S44 5LW

Accountability and Governance

The Data Protection Officer will maintain a centralised **Personal Data Breach Log**. This log will record the facts, effects, and remedial actions taken for every data incident, regardless of whether it was severe enough to report to the Information Commission. This policy and the log will be reviewed **annually** to identify systemic risks and staff training needs.

Action	Date
Adopted	10 th September 2026
Next Review Due	May 2027