

Baldons Parish Council

Data Breach Policy

Introduction

Baldons Parish Council is committed to protecting the personal data it holds about individuals, including residents, councillors, and staff. Despite best efforts, a data breach may occasionally occur. This policy sets out how the council will identify, respond to, and record data breaches in accordance with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

A prompt and well-managed response to a data breach can significantly reduce the risk of harm to those affected. All councillors and the Clerk should be familiar with this policy.

2. What Is a Data Breach

A data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Breaches can take a variety of forms, including:

- sending an email or letter containing personal data to the wrong recipient;
- loss or theft of a device containing personal data (such as a laptop or phone);
- accidental deletion of data that has not been backed up;
- an unauthorised person gaining access to council systems or files;
- posting personal data publicly (for example on a website) without authorisation;
- disclosing personal data in response to a fraudulent request.

Not all breaches will result in significant harm to individuals. However, all suspected breaches must be reported internally so that the risk can be assessed.

3. Reporting a Breach Internally

Anyone who becomes aware of a suspected or confirmed personal data breach must report it to the Clerk as soon as possible, and in any event without undue delay. If the breach involves the Clerk, it should be reported directly to the Chair of the council.

Internal reports should include:

- a description of what happened, including how the breach occurred and what data was involved;
- the date and time of the breach, or an estimate if the exact time is not known;
- the categories and approximate number of individuals affected;
- the categories and approximate volume of data involved;
- any steps already taken to contain the breach.

The Clerk will record the breach in the council's breach log (see section 7) and take immediate steps to contain it, such as recovering misdirected emails, notifying IT support, or restricting access to compromised systems.

4. Assessing the Risk

Once a breach has been reported, the Clerk must assess the likely risk to the rights and freedoms of the individuals affected. The assessment should consider:

- the type and sensitivity of the data involved;

Adopted:	September 2026	Minute:	051/26	Review date:	May 2027
----------	----------------	---------	--------	--------------	----------

Baldons Parish Council

- the number of individuals affected;
- the likelihood that the data has been accessed or used by an unauthorised person;
- the potential consequences for those individuals, such as financial loss, reputational damage, or physical harm.

This assessment will determine whether the breach must be reported to the Information Commissioner's Office (ICO) and whether affected individuals need to be notified.

5. Reporting to the ICO

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the council must report it to the ICO within 72 hours of becoming aware of the breach. This is a legal requirement under Article 33 of UK GDPR.

The 72-hour period begins when the council becomes aware that a breach has occurred - not necessarily when all details are known. If the full picture is not available within 72 hours, the council should report what it knows and provide further information as it becomes available. Breaches can be reported to the ICO online at: www.ico.org.uk/report-a-breach

The report to the ICO must include:

- a description of the nature of the breach;
- the categories and approximate number of data subjects affected;
- the categories and approximate number of personal data records affected;
- the name and contact details of the Clerk or other point of contact;
- a description of the likely consequences of the breach;
- a description of the measures taken or proposed to address the breach.

Where the council concludes that a breach does not meet the threshold for ICO notification, that conclusion and the reasoning behind it must be documented in the breach log.

6. Notifying Individuals

Where a breach is likely to result in a high risk to the rights and freedoms of the individuals affected, the council must notify those individuals directly, without undue delay. The notification should:

- describe the nature of the breach in clear, plain language;
- give the name and contact details of the Clerk as the point of contact;
- describe the likely consequences of the breach;
- describe the measures taken or proposed to address the breach and mitigate its effects;
- explain what steps the individual can take to protect themselves.

Notification to individuals may be delayed in exceptional circumstances - for example, if notifying individuals would compromise a criminal investigation - but this must be documented and agreed with the ICO where possible.

Where individual notification is not feasible (for example, because contact details are not held), the council should use other means to communicate the breach, such as a public notice.

Adopted:	September 2026	Minute:	051/26	Review date:	May 2027
----------	----------------	---------	--------	--------------	----------

Baldons Parish Council

7. Documenting Breaches

The council must keep a record of all personal data breaches, regardless of whether they are reportable to the ICO. This record (the breach log) will be maintained by the Clerk and should include:

- the date and time the breach occurred and was discovered;
- a description of the breach;
- the type and volume of data involved;
- the number of individuals affected;
- the risk assessment carried out;
- whether the breach was reported to the ICO and the date of that report;
- whether individuals were notified and the date of notification;
- the steps taken to contain and remediate the breach;
- any follow-up actions identified to prevent recurrence.

The breach log will be reviewed by the council annually as part of its data protection governance. It is an internal document and will not be routinely published.

8. Learning from Breaches

Following any breach, the Clerk will consider what steps could be taken to reduce the likelihood of a similar incident in future. This may include updating this policy, revising procedures, improving technical measures, or arranging additional training. The Clerk will report significant breaches, and any systemic issues identified, to the full council.

9. Responsibilities

The Clerk is responsible for receiving and recording internal breach reports, carrying out the risk assessment, deciding whether to notify the ICO and affected individuals, and maintaining the breach log.

The Chair is responsible for receiving breach reports that involve the Clerk, and for supporting the council in managing serious breaches.

All councillors are responsible for reporting any suspected breach they become aware of to the Clerk (or Chair) without delay.

10. Review

This policy will be reviewed annually. It will also be reviewed following any significant breach or change in ICO guidance or relevant legislation.

11. Legal and Regulatory Framework

This policy has regard to the following:

- UK General Data Protection Regulation (UK GDPR), Articles 33 and 34
- Data Protection Act 2018
- ICO guidance: Personal data breaches
- ICO guidance for local councils on data protection

Adopted:	September 2026	Minute:	051/26	Review date:	May 2027
----------	----------------	---------	--------	--------------	----------