

BRADFORD WATTS

DATA BREACH POLICY & PROCEDURE

Purpose:

The purpose of this policy is to ensure that Bradford Watts Ltd manages all personal data breaches swiftly and effectively, in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This procedure outlines how to identify, report, manage, and record data breaches, and the process for notifying the Information Commissioner's Office (ICO) and affected individuals where required.

Scope:

This policy applies to all employees, contractors, consultants, and third parties who have access to personal or sensitive information processed by Bradford Watts Ltd in any form (digital, paper, or verbal).

Definitions:

- Personal Data Breach – A security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Personal Data – Any information relating to an identified or identifiable natural person.
- Special Category Data – Data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, or data concerning a person's sex life or sexual orientation.
- Data Subject – The individual whose personal data is processed.
- Data Protection Lead (DPL) – The designated person responsible for data protection compliance within Bradford Watts Ltd.

Responsibilities:

- All Staff: Must immediately report any suspected or actual data breach to the Data Protection Lead.
- Data Protection Lead: Responsible for assessing, recording, reporting, investigating, and mitigating breaches, including liaison with the ICO and affected individuals.
- Senior Management: Ensures adequate resources and training are in place for compliance and breach management.

Version:	04
Created:	11/02/2026
Review Date:	11/02/2027

Identifying a Data Breach:

A data breach can occur through, but is not limited to:

- Loss or theft of data, devices, or documents.
- Unauthorised access to systems or personal information.
- Human error (e.g. email sent to the wrong recipient).
- Malware, ransomware, or cyber-attacks.
- Failure of security systems or improper data disposal.

Procedure for Managing a Data Breach:

Step 1 – Report Immediately:

Any employee who suspects a data breach must report it immediately to the Data Protection Lead using the internal Data Breach Notification Form. Reports should be made as soon as possible, ideally within 1 hour of discovery.

Step 2 – Contain the Breach:

The DPL will take immediate steps to contain the breach, secure systems or documents, and restrict further access.

Step 3 – Assess the Breach:

The DPL will determine if the breach is likely to result in a risk to individuals' rights and freedoms. If risk is likely, notify the ICO within 72 hours.

Step 4 – Notify the ICO (if applicable):

If a breach meets the threshold, the ICO must be notified without undue delay and within 72 hours. An initial report may be followed by updates as more information becomes available.

Step 5 – Notify Affected Individuals:

If the breach is likely to result in a high risk to individuals' rights and freedoms, notify affected individuals without undue delay, explaining what has happened and how they can protect themselves.

Step 6 – Record and Document the Breach:

All breaches must be logged in the Data Breach Register, including details, assessment, notification actions, and outcomes.

Step 7 – Review and Prevent Recurrence:

After resolution, a post-incident review will be conducted to prevent recurrence and improve processes.

Version:	04
Created:	11/02/2026
Review Date:	11/02/2027

Staff Training and Awareness:

All employees handling personal data must receive regular data protection and breach response training. Refresher sessions will be conducted annually or upon policy revision.

Disciplinary Action:

Failure to report a suspected breach or comply with this policy may result in disciplinary action in accordance with Bradford Watts Ltd's policies.

Related Policies and References:


- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- ICO Guidance: "Personal Data Breaches"
- Bradford Watts Ltd Data Protection Policy
- Bradford Watts Ltd Information Security Policy

Contact:

Data Protection Lead (DPL)
Bradford Watts Ltd
Andrew Lysandrou
Email: info@bradfordwatts.co.uk
Phone: 01992 657555

D. Pitcher MD

11.02.26



Version:	04
Created:	11/02/2026
Review Date:	11/02/2027