Data Breach Policy

Identifying, containing, reporting and learning from personal-data breaches

Version 1.0 · 03/07/2026

1. Purpose

A personal-data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This policy sets out how Swale Tutoring Service identifies, contains, records and reports breaches, and meets its obligations to the Information Commissioner's Office (ICO) and to affected individuals.

2. Scope and examples

This policy applies to all staff and to all personal data held by Swale in any form. Examples of a breach include:

- Loss or theft of a laptop, phone or paper file containing pupil or family information
- Emailing personal or safeguarding information to the wrong recipient
- Unauthorised access to accounts or files, including via a lost password or phishing
- Insecure disposal of documents containing personal data

3. Everyone's duty to report immediately

Any member of staff who becomes aware of an actual or suspected breach must report it to the Director/DSL without delay, and in any event within a few hours of discovery. Early reporting is essential to meet statutory deadlines. Staff will not be penalised for reporting a breach they may have caused, provided it is reported promptly and honestly.

4. Response procedure

Step 1 — Contain

Take immediate steps to contain the breach and recover data (for example, recall an email, change passwords, retrieve or remotely wipe a device).

Step 2 — Assess the risk

The Director/DSL assesses the likelihood and severity of risk to affected individuals, giving particular weight to any safeguarding or special-category (e.g. health, SEND) data.

Step 3 — Report to the ICO

Where the breach is likely to result in a risk to individuals' rights and freedoms, it is reported to the ICO within 72 hours of Swale becoming aware of it. If the 72-hour deadline is missed, the reasons are recorded. Reportable via ico.org.uk or 0303 123 1113.

Step 4 — Inform affected individuals

Where the breach is likely to result in a high risk, affected individuals (and, for children, their parents/carers) are informed without undue delay, in plain language, with advice on protective steps.

Step 5 — Record and learn

All breaches — reportable or not — are logged in the breach register with the facts, decisions, actions and lessons learned. The Director/DSL reviews the register to prevent recurrence.

5. Safeguarding data

A breach involving safeguarding information is treated as high priority. Where such a breach could increase risk to a child, the DSL considers whether a safeguarding referral is also required (see Safeguarding & Child Protection Policy).

6. Records and review

The breach register is retained in line with the Data Retention & Erasure Policy. This policy is reviewed annually or after any significant breach.

Approved by Shelley Wilson, Director & Designated Safeguarding Lead.
Version 1.0 · Approved 03/07/2026 · Reviewed annually.