# Telford Court

## Breach Notification Policy and Procedure

## 2026-2027

## 1. Policy Statement

The Greenhouse HyFlex Academy is committed to handling personal data responsibly and in compliance with UK GDPR and the Data Protection Act 2018. In the event of a personal data breach, The Greenhouse will respond promptly, contain the breach, assess the risk, and notify the appropriate authorities and individuals where required.

## 2. Legal Framework

This policy complies with:

- UK GDPR — Articles 33 and 34 (notification of breaches)
- Data Protection Act 2018
- The Data Use and Access Act 2025
- ICO Breach Reporting Guidance
- Keeping Children Safe in Education 2026

## 3. What is a Personal Data Breach?

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Sending an email containing personal data to the wrong recipient
- Loss or theft of a device containing personal data
- Unauthorised access to systems holding personal data
- Accidental deletion of personal data without backup
- A cyber attack resulting in data exposure

## 4. Roles and Responsibilities

**Data Protection Lead / Headteacher**

- Overall responsibility for breach management and notification
- Decision-maker on whether to report to the ICO or notify individuals

**All Staff**

- Must report any suspected or actual breach to the Headteacher immediately — without delay
- Must not attempt to investigate or resolve a breach without reporting it first

## 5. Breach Response Procedure

**Step 1 — Identify and Report**

Any staff member who becomes aware of a potential breach must report it to the Headteacher immediately by phone or in person, and in writing as soon as practicable.

**Step 2 — Contain**

The Headteacher will take immediate steps to contain the breach, including:

- Preventing further access or distribution
- Recovering lost data where possible
- Securing compromised systems

**Step 3 — Assess**

The breach will be assessed to determine:

- The type and volume of data affected
- The likely consequences for individuals (risk of harm)
- Whether the breach is reportable to the ICO

**Step 4 — Report to the ICO (where required)**

If the breach is likely to result in a risk to the rights and freedoms of individuals, it must be reported to the ICO within 72 hours of becoming aware. Reports are made via the ICO online portal.

**Step 5 — Notify Individuals (where required)**

If the breach is likely to result in a high risk to individuals, those individuals must be notified directly without undue delay.

**Step 6 — Record and Review**

All breaches must be recorded in the Breach Register, regardless of whether ICO notification is required. A post-incident review will identify lessons learned and any preventative actions required.

## 6. The Breach Register

The Greenhouse maintains a Breach Register recording all personal data breaches, including those that are not reportable. The register includes:

- Date and time the breach was identified
- Nature of the breach and data affected
- Actions taken to contain and remediate
- Whether reported to the ICO and/or individuals
- Outcome and lessons learned

## 7. Monitoring and Review

This policy will be reviewed annually by the Headteacher and approved by the Business Director.

## 8. Related Policies

This policy must be read in conjunction with the following related policies:

- UK GDPR Policy and Procedure
- Archiving, Disposal and Storage of Records Policy
- Subject Access Request Policy and Procedure

**This policy has been written by Fiona Conde (Headteacher) and approved by Jonathon Simpson (Business Director).**

Approval Date: June 2026
Review Date: June 2027