Data breach reporting

1. Purpose

The purpose of this Data Breach Reporting Policy is to establish clear procedures for detecting, reporting, and managing personal data breaches at Turning Point Leeds (TPL). The policy ensures compliance with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018, protecting individuals' rights and freedoms while maintaining trust within our community.

2. Definitions

- Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
- Data controller: Turning Point Leeds, responsible for determining the purposes and means of processing personal data.
- Data processor: Any third party engaged by TPL to process personal data on its behalf.

3. Responsibilities

- Directors also DPO: Oversees the breach response process, ensures GDPR compliance, and acts as the main contact for the Information Commissioner's Office (ICO).
- Directors: ensure resources are allocated to manage and mitigate breaches effectively.
- Employees and volunteers: Must report any actual, suspected, or "near miss" breaches immediately to the DPO/Director.

4. Detection and Assessment

- Detection: Breaches may be detected through system monitoring, staff vigilance, reports from parents/pupils, or alerts from third-party providers.
- Initial assessment: Once reported, the DPO will log the incident and carry out a rapid risk assessment to determine its severity, scope, and potential impact.

5. Reporting Procedure

- Internal reporting: Staff must report suspected breaches immediately, providing:
    - What happened (description of the breach)
    - Date/time of occurrence or discovery
    - Nature of data involved
    - Who may be affected
    - Any initial containment steps taken
- Host school notification: Where the breach involves pupil data, the host school will be informed without delay and updated throughout the investigation.
- DPO response: The DPO will acknowledge receipt, investigate further, and decide whether the breach must be reported to the ICO and/or affected individuals.

6. Response and Mitigation

- Containment: Immediate action will be taken to stop or limit the breach (e.g., suspending compromised accounts, securing physical records).
- Investigation: A full inquiry will establish the cause, scale, and potential risks.
- Notification of individuals: Where there is a high risk to rights or freedoms, pupils, parents/carers, and staff will be informed without undue delay.
    - Notifications will explain what happened, the data involved, likely consequences, and steps individuals can take to protect themselves.
- ICO notification: If required, the ICO will be notified within 72 hours of awareness, in line with statutory guidance.
- Restorative response: TPL will work openly with affected individuals, host schools, and families to rebuild trust, explain lessons learned, and demonstrate changes to prevent recurrence.

7. Record-Keeping

- All breaches, whether reported to the ICO or not, will be recorded in TPL's Data Breach Log.
- Records will include details of the breach, actions taken, risk assessment, outcomes, and any communication with external bodies.
- Logs will be reviewed termly to identify trends and strengthen preventative measures.

8. Training and Awareness

- All staff will receive training at induction and annually on:
    - Recognising potential breaches
    - How to report concerns quickly and clearly
    - Their responsibilities for handling personal data securely
- Refresher training will be provided after any significant breach.

9. Review and Updates

This policy will be reviewed annually or following a serious incident to ensure compliance with legal requirements and best practice. Lessons learned from breaches will inform future training, processes, and system improvements.

Conclusion

TPL takes data protection seriously and is committed to responding promptly, effectively, and transparently to any data breaches. By following this policy, we will protect the privacy of individuals, comply with GDPR, and uphold the confidence of pupils, parents/carers, staff, and host schools.

Written: August 2025

Next Review: August 2026