Policy – Data Breach Policy and Procedure			
Document Reference No. 18	**Revision Level: 0**	**Approved By:**	
References: Operational		**Originator:** CEO	**Date Approved:** 22/9/2025

1. Purpose

The purpose of this policy is to ensure that Trauma Informed Parenting responds effectively to data breaches, minimising impact, ensuring legal compliance, and protecting personal data.

2. Scope

This policy applies to all staff, volunteers, trustees, and third parties handling personal data within Trauma Informed Parenting. It covers breaches involving:

- **Personal data leakage or unauthorised access.**
- **Cyber-attacks or security failures impacting confidentiality.**
- **Loss or theft of devices containing sensitive information.**
- **Accidental or unlawful disclosure of personal data.**

3. Policy

3.1 Data Breach Response Principles

Trauma Informed Parenting commits to the following:

- Swift detection, assessment, and containment of breaches.
- Transparent communication with affected individuals and regulatory bodies.
- Investigation of root causes and prevention of future incidents.
- Compliance with UK GDPR requirements, including ICO reporting obligations.

3.2 Lawful Basis for Reporting Data Breaches

Trauma Informed Parenting will report data breaches when:

- The breach poses a risk to individuals' rights and freedoms (UK GDPR Article 33).
- Personal data has been exposed, stolen, or misused.
- The breach meets ICO thresholds for mandatory reporting within 72 hours.

4. Procedure

4.1 Detection and Identification

- Identify the breach through internal monitoring or external alerts.
- Log incident details, including time, nature, and systems affected.
- Notify key personnel, including IT security, legal advisors, and senior management.

4.2 Containment and Assessment

- Limit further exposure by securing affected systems and disabling compromised accounts.
- Assess the scope, determining which data has been impacted.
- Engage external cybersecurity support, if necessary, for deeper forensic investigation.

4.3 Notification & Reporting

- Inform affected individuals promptly, explaining the breach and steps they can take.
- Report to the Information Commissioner's Office (ICO) within 72 hours, if legally required.
- Maintain internal communication, ensuring all team members understand next steps.

4.4 Investigation and Recovery

- Conduct a formal investigation to determine the cause and impact of the breach.
- Document findings, outlining mitigation efforts and lessons learned.
- Restore systems, applying strengthened security measures before resuming normal operations.
- Provide support to affected individuals, where necessary.

4.5 Review and Prevention

- Evaluate the response to identify improvements in breach management.
- Enhance security protocols, including encryption, staff training, and system monitoring.

5. Monitoring and Review

This policy will be reviewed annually, ensuring alignment with UK GDPR, ICO guidelines, and evolving cybersecurity risks.

Revision Level.	Description of Revision	Approved	Date

		By: S Scott22/ 9/25	
0	Approved on	**Board**	22/9/26
1	**Reviewed**		

6.0 Related Procedure

19-Data Protection

2-Confidentiality Policy

48-Safeguarding Policy

1-Code of Conduct Policy

35-Whistleblowing Policy