

Different Minds (ADHD-ASD Norfolk) Ltd

Data Breach and Governance Breach Reporting Policy

1. Purpose

The purpose of this policy is to outline the procedures Different Minds (ADHD-ASD Norfolk) Ltd will follow in the event of a data protection breach or governance breach, in accordance with UK data protection legislation and NHS contractual requirements. This includes the requirement to report notifiable breaches to the relevant NHS Commissioner and other regulatory bodies, such as the Information Commissioner's Office (ICO), where appropriate.

2. Scope

This policy applies to all staff members, volunteers, sub-contractors, and third parties working on behalf of Different Minds (ADHD-ASD Norfolk) Ltd who have access to personal, confidential, or sensitive data.

3. Definitions

- **Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Governance Breach:** A breach of organisational, contractual, or regulatory obligations relating to the handling of data or the provision of services under NHS contracts.
- **Notifiable Breach:** A breach that is likely to result in a risk to the rights and freedoms of individuals, which must be reported to the ICO and, where applicable, the NHS Commissioner.

4. Legal and Regulatory Framework

This policy is underpinned by:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- NHS Data Security and Protection Toolkit
- The Common Law Duty of Confidentiality
- Relevant NHS England and NHS Commissioner reporting requirements

5. Roles and Responsibilities

- **Data Protection Officer (DPO):** Responsible for investigating breaches, advising on mitigation, and leading on any necessary reporting.
- **All Staff and Sub-Contractors:** Responsible for reporting actual or suspected breaches immediately and assisting with investigations.
- **Senior Management:** Ensures breaches are escalated and managed appropriately in line with policy and legal requirements.

6. Identification and Reporting of Breaches

All suspected or actual breaches must be reported **immediately** upon discovery to the Data Protection Officer or designated senior manager. This includes but is not limited to:

- Unauthorised access to personal data

- Loss or theft of data or equipment containing data
- Emailing personal data to the wrong recipient
- Failure to securely dispose of confidential information
- Any unauthorised sharing of NHS data

7. Incident Investigation and Documentation

- The DPO will assess the severity and impact of the breach within **72 hours** of notification.
- An internal investigation will be conducted and documented using the organisation's Incident Reporting Form.
- Where a breach is deemed notifiable, it will be reported via the **NHS DSPT Incident Reporting Tool** and, if required, to the **ICO** and the relevant **NHS Commissioner**.

8. Reporting to NHS Commissioners

Where the breach involves data related to services commissioned by the NHS:

- The NHS Commissioner will be informed as soon as practicably possible following initial assessment.
- A full breach report, including root cause analysis, risk assessment, and remedial actions, will be submitted in line with NHS contractual obligations.
- Ongoing updates will be provided to the Commissioner until the matter is resolved.

9. Communication and Remediation

- Where individuals are affected, they will be informed in a timely, clear, and supportive manner.
- Appropriate remedial measures will be implemented to reduce the risk of reoccurrence.
- Staff training, system updates, or policy changes may be implemented as part of corrective actions.

10. Record Keeping

A full record of all breach incidents, investigations, outcomes, and reports will be maintained securely by the DPO for a minimum of six years.

11. Policy Review

This policy will be reviewed annually or following any serious incident, changes in legislation, or updates to NHS requirements.

Approved by:

Graham Boulter MSc

Director

Different Minds (ADHD-ASD Norfolk) Ltd

3/4/25 to be reviewed 3/4/26