

Different Minds (ADHD-ASD Norfolk) Ltd
NHS Data Security and Protection Toolkit & Audit Procedure Policy

1. Purpose

This policy outlines the commitment of Different Minds (ADHD-ASD Norfolk) Ltd to uphold the highest standards of data security and confidentiality, in accordance with the requirements of the NHS Data Security and Protection Toolkit (DSPT). It also sets out the audit procedures in place to monitor compliance and ensure continuous improvement in data protection practices.

2. Scope

This policy applies to all staff, volunteers, and sub-contractors who have access to personal, sensitive, or confidential information within the organisation, including information relating to clients, service users, employees, and partners.

3. Policy Statement

Different Minds (ADHD-ASD Norfolk) Ltd is committed to safeguarding all personal and sensitive information by:

- Fully complying with the NHS Data Security and Protection Toolkit.
- Maintaining secure systems and procedures for data processing, storage, access, and disposal.
- Ensuring all staff and contractors are trained and aware of their data protection responsibilities.
- Regularly auditing and reviewing practices to maintain compliance and protect data integrity.

4. The Data Security and Protection Toolkit (DSPT)

The DSPT is a self-assessment and compliance tool designed by NHS Digital to support organisations in handling data safely and securely.

Different Minds (ADHD-ASD Norfolk) Ltd commits to:

- Completing and publishing the DSPT assessment annually.
- Meeting all mandatory evidence and standards within the toolkit.
- Acting upon any identified areas for improvement through documented action plans.

5. Responsibilities

- **The Data Protection Officer (DPO)** is responsible for overseeing data protection strategy and compliance.
- **Senior Management** is responsible for ensuring the organisation meets its DSPT obligations.
- **All staff and contractors** must complete annual data security training and adhere to data protection policies and procedures.

6. Training

All staff and sub-contractors are required to undertake mandatory Data Security Awareness training annually, as outlined in the DSPT. Completion is monitored and recorded.

7. Audit Procedure

To ensure continuous compliance and improvement:

- Regular internal audits of data protection practices will be conducted at least annually.
- Spot checks may be carried out to ensure adherence to data handling procedures.
- Audit findings will be documented, and actions will be tracked through an improvement log.
- Any incidents, near misses, or data breaches identified during audits will be reported in line with the organisation's Incident Management Policy and, if necessary, to the Information Commissioner's Office (ICO).

8. Data Security Measures

The organisation will implement appropriate technical and organisational controls, including but not limited to:

- Secure access controls and password protection
- Encrypted devices and secure file transfer methods
- Regular data backups and secure storage
- Controlled data retention and disposal procedures

9. Breach Reporting

Any actual or suspected data breaches must be reported immediately to the Data Protection Officer. Where necessary, breaches will be reported via the DSPT portal in line with NHS and ICO guidance.

10. Review

This policy will be reviewed annually or sooner if required due to legislative changes, audit findings, or updates to the DSPT framework.

Approved by:

Graham Boulter MSc

Director

Different Minds (ADHD-ASD Norfolk) Ltd

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