Remarkable Autism Ltd

The Autism Specialists

Data Breach Policy

February 2025

Remarkable Autism Ltd
449 Wargrave Road
Newton-Le-Willows
Merseyside
WA12 8RS

01925 224 899

enquiries@remarkable-autism.org

www.remarkable-autism.org

Remarkable

Reviewer:	IT Manager
Co-Reviewer:	Deputy CEO
Updated:	February 2025
Next Review:	February 2028
Committee:	Finance & Business Resources
Approved by the full Governing Body/Board of Trustees:	03.02.25

This policy should be read in conjunction with the following policies:	
1	Data Protection
2	Data Retention
3	Cyber Security

Contents

Policy Overview

Purpose: This policy outlines Remarkable Autism's approach to identifying, managing, and preventing personal data breaches in compliance with the UK GDPR and associated data protection legislation.

Scope: This policy applies to all personal data processed by Remarkable Autism Ltd and is mandatory for all staff, trustees, and governors.

Principles

Compliance: Ensure legal obligations for data protection and breach management are met.

Accountability: Define clear roles and responsibilities for managing breaches.

Transparency: Communicate effectively with stakeholders when breaches occur.

Policy

Definitions

Personal Data: Any information that relates to an identified or identifiable individual. Examples include names, email addresses, identification numbers, and online identifiers like IP addresses. Personal data can also include opinions or behavioural information, provided it can be linked to an individual.

Special Category Data: Previously called "sensitive personal data," this includes information about a person's racial or ethnic origin, political or religious beliefs, health data, sexual orientation, biometric data, and criminal convictions. These types of data require extra care under the UK GDPR.

Personal Data Breach: A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include:

- Sending sensitive information to the wrong email address.
- Losing a device that contains unencrypted personal data.
- Experiencing a cyberattack or phishing scam that exposes data.

Data Subject: The individual whose personal data is being processed. For example, students, staff, governors and trustees whose details are held by the organisation.

ICO (Information Commissioner's Office): The UK's independent authority responsible for enforcing data protection laws. The ICO must be notified of certain breaches within 72 hours.

Responsibility

Role	Responsibility
IT Manager	Primary responsibility for breach notifications, coordinating responses, and maintaining records.
Deputy CEO	Secondary point of contact for data breach management in the IT Manager's absence.
CEO	Overall responsibility for Remarkable Autism, ensuring that effective policies, resources, and oversight mechanisms are in place to support compliance and response efforts.
Data Protection Officer (DPO)	Provides oversight, ensures compliance, and liaises with the ICO as needed.
Staff, governors and Trustees	Report suspected breaches promptly and assist in investigations as required.

DPO Contact Details:
Judicium Consulting Limited
72 Cannon Street, London, EC4N 6AE
dataservices@judicium.com
www.judiciumeducation.co.uk
0203 326 9174
Lead Contact: Craig Stilwell

What is a Personal Data Breach?

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

Appendix A.

Data Breach Procedure

When does it need to be reported?

Report any suspected breach immediately.

Reporting a Data Breach

Complete the Data Breach Reporting Form (Appendix B.) and submit it to the IT Manager. The IT Manager will then notify the appropriate parties which may include line managers, SLT or the DCEO/CEO.

Managing & Recording the Breach

Collectively, the IT Manager and DPO will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to: -

- **Containment**: Limit the scope of the breach to prevent further data loss or exposure.
- **Assessment**: Evaluate the nature of the breach, the data affected, and the potential impact.
- **Recording**: Document details in the Data Breach Register, including dates, actions taken, and outcomes.

Notifying the ICO

- Notify the ICO within 72 hours if the breach poses a risk to individuals' rights and freedoms.
- Include the nature of the breach, data categories affected, and mitigation measures.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the IT Manager will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures Remarkable Autism Ltd have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, IT Manager will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

Notifying Other Authorities

Inform relevant parties such as insurers, local authorities, or police, depending on the nature of the breach.

Assessing the Breach

Once the initial reporting procedures are complete, Remarkable Autism Ltd will conduct a thorough assessment of the breach to determine its severity and required actions. The following factors will be considered:

Type of Data Involved:

- Is the data personal or special category data?
- How sensitive is the data (e.g., health records vs. general contact details)?

Volume of Data:

- How many records or individuals are affected?

Affected Individuals:

- Who is impacted (e.g., staff, students, external stakeholders)?
- Are there vulnerable individuals involved, such as children?

Potential Consequences:

- What harm could result from the breach (e.g., financial loss, identity theft, or reputational damage)?
- Are there any risks to physical safety or privacy?

Mitigation Measures:

- Are there protections in place to minimize harm (e.g., encryption, pseudonymisation)?
- What steps can be taken immediately to contain the breach?

Likelihood of Recurrence:

- Are systemic issues (e.g., process gaps, lack of training) contributing to the breach?
- Are similar breaches likely without corrective actions?

The findings of this assessment will determine whether the ICO, affected individuals, or other authorities need to be notified. All assessment details will be recorded in the Data Breach Register.

Preventing Future Breaches

- Review and update technical and organisational measures regularly.
- Provide ongoing training for staff to recognise and mitigate data security risks.
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing activities.
- Debrief management and trustees after significant breaches to improve practices.

Reporting Data Concerns

Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the IT Manager or the DPO. This can help capture risks as they emerge, protect Remarkable Autism Ltd from data breaches and keep our processes up to date and effective.

Training

Remarkable Autism Ltd will ensure that staff, trustees and governors are aware of the need to report data breaches to ensure that they know how to detect a data

breach and the procedures of reporting them. The IT Manager will review this document annually and ensure training is provided through a selection of channels, including awareness months and formal training courses through our current provider.

Monitoring

The policy will be updated if legislative changes occur.

Appendix B.
Data Breach Reporting Form

- Consult with your line manager if assistance is needed to complete the form.
- Once reported, you should not take any further action in relation to the breach. You must not notify any affected individuals or investigate further. The IT Manager will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

This form is to be completed by staff when a data breach is suspected. Please provide as much detail as possible and submit the completed form to the IT Manager without delay. If unsure about any section, seek assistance from your line manager or the IT Manager.

Data Breach Form