Remarkable

Autism. Redefining what's possible.

Cyber Security Policy

August 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:	Head of Business Resources
Updated:	August 2025
Next Review:	August 2027
Committee:	Finance and Business Resources
Approved by the full Governing Body/Board of Trustees:	15.09.25

This policy should be read in conjunction with the following policies:	
1	Data Protection Policy
2	Data Retention Policy
3	Data Breach Policy
4	Acceptable Use of IT Policy

Change History Record

Current Version	**Previous Version**	**Summary of changes made**	**Section Heading & Page Number**
Sept 2025	Sept 2023	Updated definition of cyber-crime to include mobile devices	Section 3
Sept 2025	Sept 2023	Reporting lines updated - incidents now reported to IT Manager with escalation to DPO	Section 4 / Appendix A2
Sept 2025	Sept 2023	Policy restructured - split into high-level Policy and detailed Procedures appendix	Whole document
Sept 2025	Sept 2023	Added GDPR compliance statement	Section 4

Contents

Introduction

Cyber security has been identified as a key risk for the Charity. Every employee, volunteer, and contractor has a role in protecting data and systems. The Charity has invested in technical cyber security measures, but vigilance and responsible behaviour from staff are equally essential.

Trustees are responsible for the oversight of compliance and assurance, enabling resources are sufficient to minimise risk and respond to incidents appropriately if they arise.

The Senior Leadership Team are responsible for the implementation of safe systems, training for all ICT users, promoting a culture of awareness and coordinating any incident response with the assistance of the IT Manager.

The IT Manager is responsible for the operational management of cyber security. Breaches of this policy may lead to disciplinary action.

Purpose and Scope

This policy sets out the Charity's commitment to:

- Preventing cyber-crime through appropriate systems, training, and controls.
- Responding effectively to incidents to minimise harm via the Cyber Incident Response Plan.
- Ensuring compliance with legal and regulatory requirements.

It applies to all staff, trustees, governors, contractors, volunteers, and learners who use the Charity's ICT systems.

What is Cyber-Crime?

Cyber-crime is criminal activity carried out using computers, mobile devices, or the internet. Examples include but are not limited to:

- Hacking, phishing, or social engineering
- Malware, viruses, or ransomware
- Attempted identity theft or email spoofing

Potential consequences of cyber-crime include:

- Financial loss
- Breach of confidentiality and data protection
- Regulatory penalties

- Reputational damage
- Business interruption
- Structural or financial instability

Policy Statements

- The Charity will maintain appropriate technical and organisational measures to protect systems and data.
- Staff must follow all related policies and attend cyber security training.
- Staff must report suspected breaches or mistakes immediately to the **IT Manager**, who will escalate to the **Data Protection Officer (DPO)** as required.
- Charity data must only be stored in approved systems (e.g. Microsoft 365). Temporary local copies must be deleted promptly after use.
- Personal use of ICT systems must be minimal and must never compromise security or safeguarding.
- The Charity will review this policy every two years or sooner following a major incident or regulatory update.
- This policy operates in line with UK GDPR and the Data Protection Act 2018. Where a cyber incident involves personal data, GDPR reporting and accountability requirements will take precedence.

Policy Impact

-
- We have a rolling programme for reviewing our Company policies. We regularly review the impact of our policies on the needs, entitlements and outcomes for students, service users, staff and parents.

Appendix A - Procedures

A1. Technical Measures in Place

- Firewalls, anti-virus and anti-spam software
- Real-time security updates and patching
- URL filtering and web protection
- Encrypted data backup (local and cloud)
- Encryption of devices
- Account and software lifecycle management (removal of unused accounts/software)
- Password policies and multi-factor authentication (MFA)
- Software installation restrictions via Group Policy
- Phishing simulation and staff training
- Email protection (SPF, DKIM, DMARC)
- Access controls and permissions management

A2. Staff Responsibilities

- Use strong, unique passwords and keep them secret.
- Never share login details or reuse passwords.
- Do not disable or bypass security measures.
- Report breaches, mistakes, or suspicious activity immediately to the IT Manager.
- Use Charity-issued devices where possible; personal devices may only connect to Guest Wi-Fi.
- Do not install software without IT Manager approval.
- Avoid clicking on unknown links or attachments.
- Do not misuse ICT systems (e.g. illegal activity, accessing inappropriate content, or removing data without permission).

A3. Incident Management Process

1. Containment and recovery as detailed in the Cyber Incident Response Plan - investigate, mitigate damage, and recover data.
2. Assessment of risk - identify what was affected, how sensitive it was, and the potential impact.
3. Notification - consider reporting to ICO, insurers, trustees, and stakeholders as appropriate.
4. Evaluation and response - learn lessons and strengthen controls.

If the incident involves personal data, the **Data Breach Procedure** will be followed.

A4. Training and Awareness

- Cyber security training will be provided at induction and refreshed periodically.
- Additional training will be delivered where significant new threats are identified, laws/policies change, or following an incident.