Remarkable Autism Ltd

The Autism Specialists

Cyber Security Policy

September 2023

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:	*Technical Support Manager*
Co-Reviewer:	*Deputy CEO*
Updated:	*September 2023*
Next Review:	*September 2025*
Committee:	*Finance and Business Resources*
Approved by the full Governing Body/Board of Trustees:	*December 2021*

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

Contents

Introduction....4
Purpose and Scope....4
What is cyber-crime?....4
Cyber-crime prevention....5
Technology solutions....5
Controls and guidance for staff....6-7
Cyber-crime incident management process....7-8
Policy Impact....8

Introduction

Cyber security has been identified as a risk for the organisation and every employee needs to contribute to ensure data security.

The organisation has invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the organisation's IT systems.

The Technical Support manager is responsible for cyber security within the organization.

As an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our [Data Protection Policy, Data Breach Policy, Data Retention Policy, and Acceptable Use of IT policy.

Purpose and Scope

The purpose of this document is to establish systems and controls to protect the organisation from cyber criminals and associated cyber security risks, as well as set out an action plan should the organisation fall victim to cyber-crime. This policy is relevant to all staff.

What is cyber-crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet, including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect organisations and/or individuals: -

- financial
- Confidentiality and data protection;
- Potential for regulatory breach;
- Reputational damage;
- Business interruption; and
- Structural and financial instability.

It is important, given the serious consequences above, to be careful not to fall victim of cyber-crime and to follow the guidance within this policy.

Cyber-crime prevention

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Technical Support Manager can provide further details of other aspects of the organisation risk assessment process upon request.

The Organisation has put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance to staff.
It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

Technology solutions

The Organisation have implemented a variety of technical measures in place for protection against cyber-crime. They include:

(i) Firewalls;
(ii) Anti-virus and anti-spam software;
(iii) Auto or real-time updates on our systems and applications;
(iv) User level URL filtering;
(v) Secure, encrypted data backup (local and cloud based. Local disks removed offsite and stored in a fireproof box);
(vi) Encryption;
(vii) Deleting or disabling unused/unnecessary user accounts;
(viii) Deleting or disabling unused/unnecessary software;
(ix) Using strong passwords;
(x) Restricting software installations through group policy.
(xi) Disabling auto-run features;
(xii) Phishing simulation software & training.
(xiii) Configuring SPF, DKIM and DMARC on our email system (anti-tamper and anti-email spoofing protocols, they prevent someone outside Wargrave House sending emails as if they belong to Wargrave House);
(xiv) Using Multi factor Authentication where possible; and
(xv) Multiple levels of user access controlled by Access Control Lists (Windows Permissions).

It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

Controls and guidance for staff

(a) All staff must follow the policies related to cyber-crime and cyber security as listed on page 2 this policy.

(b) All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the Organisation or any third parties with whom we share data.

(c) All staff must:

(i) Choose strong passwords (the Organisation's IT team advises that a strong password contains at least three of the following four character sets:

- Lowercase alpha characters (e.g. a, b, c, d, e)
- Uppercase alpha characters (e.g. A, B, C, D, E)
- Numbers (e.g. 1, 2, 3, 4, 5)
- Special symbol or punctuation characters (e.g. ! @ # $ % & * _ + ~ . ,>).

Space characters are allowed in a Windows password but you should avoid using them at the beginning and end of a password.

(ii) Keep passwords secret;
(iii) Never reuse a password;
(iv) Never allow any other person to access the organisation's systems using your login details;
(v) Not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the organisation's IT systems;
(vi) Report any security breach, suspicious activity, or mistake made that may cause a cyber-security breach, to the Office and Communication's Manager (responsible for GDPR) as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our data breach policy;
(vii) Where possible, access work systems using computers or phones that the organisation owns. Staff/Students may only connect personal devices to the Guest Wi-Fi provided;
(viii) Not install software onto your organisation devices. All software requests should be made to the Technical Support Manager;

(ix) Avoid clicking on email attachments or links to unknown websites, downloading large files, or accessing inappropriate content using the organisation's equipment or networks.

(d) All staff must not misuse IT systems. The organisation considers the following actions to be a misuse of its IT systems or resources:

(i) Any malicious or illegal action carried out against the organisation or using the organisation's systems;
(ii) Accessing inappropriate, adult or illegal content within the organisation's premises or using the organisation's equipment;
(iii) Personal use of organisation's IT systems during working hours unless permission is granted by your line manager;
(iv) Removing data or equipment from organisation's premises or systems without permission, or in circumstances prohibited by this policy;
(v) Using the organisation's equipment in a way prohibited by this or the Acceptable Use of IT Policy;
(vi) Circumventing technical cyber security measures implemented by the organisation's IT team; and
(vii) Failing to report a mistake or cyber security breach.

More detailed information can be found in our Acceptable Use of IT Policy.

Cyber-crime incident management process

The incident management process consists of four main stages:

- **Containment and recovery** to include investigating the breach and utilising appropriate staff and external expertise (through our cyber insurance policy) to mitigate damage and recover any data loss where possible.

- **Assessment of the ongoing risk** to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.

- **Notification** to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents/cyber insurance company as appropriate.

- **Evaluation and response** to consider any improvements to data security and evaluate future threats to security.

Where it is apparent that a cyber-security incident involves a personal data breach, the organisation will invoke their Data Breach procedure rather than follow out the process in section 5.

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.