ALL TOGETHER, MORE SUPPORT

Cyber Security Policy

TABLE OF CONTENTS

INTRODUCTION

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Vista Wellbeing CIC has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

PURPOSE

The purpose of this policy is to (a) protect Vista Wellbeing's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

SCOPE

This policy applies to all of Vista Wellbeing's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware. Mention of "employees" in this document is also intended to cover volunteers

CONFIDENTIAL DATA

Vista Wellbeing CIC defines "confidential data" as:

- Unreleased financial information.
- Client, supplier, and stakeholder information.
- Project and sales-related data.
- Business processes, and/or new technologies.
- Employees' passwords and personal information.
- Company contracts and legal records.

Vista Education, in addition to the above, "confidential data" as:

- Student data such as financial and payment information and registration data
- Restricted data such as Specific Assessment Guidance [SAG] documents and Cirrus assessment materials
- SAGs will be password protected at the point of download

DEVICE SECURITY

COMPANY USE

To ensure the security of all company-issued devices and information, Vista Wellbeing employees are required to:

- Keep company-issued devices, including tablets, computers, and mobile devices, password-protected (in line with device or industry minimum expectations).
- Secure all relevant devices before leaving them unattended.
- Obtain authorisation from a Vista Wellbeing Director before removing devices from company premises.
- Allow regular updates for software and hardware, including all security and anti-virus updates

PERSONAL USE

Vista Wellbeing CIC recognises that employees may be required to use personal devices to carry out work tasks. To ensure systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

EMAIL SECURITY

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software. Therefore, Vista Wellbeing CIC requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact a Vista Director regarding any suspicious emails.

TRANSFERRING DATA

Vista Wellbeing CIC recognises the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we will:

- Only transfer confidential data using suitably secure methods. This may include, for example, using an encrypted email service such as TLS (used by Gmail and Outlook). It may also require attachments to be password protected.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Immediately alert a Vista Wellbeing Director of any breaches, malicious software, and/or scams.

DATA SECURITY

Vista Wellbeing CIC's policy is that all critical data should be backed up using one or more of the following:

- Remote storage on Google Drive or One Drive
- Local storage via a second external Hard Drive or Time Machine (Mac)

When using USBs to transfer data, these should be safely stored and any sensitive files must be password protected. USBs must be tracked and returned so that they are not left unaccounted for.

VIRUS PROTECTION

Vista Wellbeing CIC requires all PCs and laptops to have appropriate anti-virus protection installed and active.

ONLINE PASSWORDS

Passwords relating to online banking must NEVER be stored.

Other passwords (such as Gmail accounts) may be stored using an encrypted service such as that which comes as part of Chrome.

IMPORTANT

Vista Wellbeing CIC has several shared laptops. It is essential that all personal profiles are logged out of before sharing a device. If personal profiles are enabled and open it is possible that the autofill password function could be available to unauthorised parties.

SPECIFIC SITES

MemberMojo's security policy can be found here: https://membermojo.co.uk/vista/help/security

One Drive's data safety information can be found here: https://support.microsoft.com/en-gb/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1

This policy will be reviewed annually by the Board of Directors

Next Review Date: January 2027