Information and Technology Security Policy

Contents

Overview

At Genius Within CIC ("the Company") we use a number of IT systems and collect various types of information in order to fulfil the needs of customer and client projects.

It is worth noting that any client details, because of the nature of our business, are considered 'medical data' and therefore subject to the most severe penalties in the event of a data breach, loss, or technology failure. So, as with the GDPR and data security policies, we must pay due diligence to keeping our clients' safe and follow these instructions to the letter.

Purpose

To ensure that the security of our data and staff is absolutely paramount in our day to day actions. We are responsible for making sure all data is secure at all times and that we as individuals we are keeping ourselves safe and the company. Therefore in the following policy are guidelines, best practices and what can and cannot be done with our systems and data.

Scope

This is a mandatory policy and associated guidelines apply to all employees, associates and Tier 1 Suppliers who have access to or are responsible for our data and/or systems and in accordance with our Information and Technology Virus Detection Plan and GDPR Policy.

Policy

Responsibility

The Leadership Team is responsible for monitoring the Information and Technology systems in use at Genius Within.

However, it is the responsibility of all systems users to follow this policy and associated guidelines. We are all required to report any activity that could or has caused a security breach to our premises or systems. Any issues found will be reported immediately to a Director who will assess the relevant corrective actions.

Corrective actions will be implemented pending a full investigation and identification information and any associated technology will be audited periodically as part of the reviews of our Quality Management System. Any non-conformity or breach will be reported to the Leadership Team who will manage the incident reporting process until the issue is resolved.

Data Protection

The Company needs to collect and use certain types of information about its employees, associates, customers, and end-user clients in order to carry out its legitimate business purposes. Any personal data that is kept is done so securely in our HR and Operations Databases.

We collect only the data necessary to the purpose of conducting our business and only use it for administration and customer service activities, as detailed in our GDPR Policy.

All documents and data are controlled by our Quality Management System processes:

document and data – describes how documents are to be prepared, identified and stored

control of records – details where documents and records are to be stored, for how long and how they will be disposed of

Customer specified document and data retention guidance will be applied where defined as part of a customer project.

Clear Desk Policy

The Plumpton and Birmingham offices maintain a clear desk policy to ensure that confidential information cannot be accessed, however inadvertently, by unauthorised personnel.

At the end of each day, or when desks/offices are unoccupied, any 'confidential' information must be locked away. All computers and laptops should be locked when unoccupied

All wastepaper, which has any personal or confidential information or data on, must be disposed of in the shredded bin at the end of the day. Under no circumstances should this type of wastepaper be thrown away with normal rubbish in the wastepaper bins

Clear screen - all computers have an auto timeout function activated to lock the computer after more than 10 minutes of inactivity.

Screen lock must be activated every time you leave your PC/Laptop/ Other device unattended.

Home Working

It is important that company laptops are shut down completely when not in use. This is to protect confidentiality and improve the performance and lifespan of the machine.

Video Calls

It is important to be aware of extra security considerations when using video communication platforms such as Zoom, or Microsoft Teams

No documentation, images or personal information may be shared through video calls.

No personal or identifiable data is shared with any other participant using a video call.

Employees and Associates must use applications responsibly, appropriately, and safely at all times, and ensure no children are present during the video calls.

Video calls must be made in a neutral space and users must ensure that there is nothing in view that identifies individuals or family members or where they live. Documentation belonging to the company must be kept out of view of unauthorised users.

Employees and Associates are trusted to dress as they would for normal face to face delivery whether office or community venue setting and be professional always.

You must only use the Genius Within authorised platforms for video calls and never download additional tools to devices without seeking advice and permission first.

You can only use Genius Within devices (or devices authorised by the company, such as Shaw Trust laptops and phones) to access video calls, email, SMS and phone calls.

Internal Systems – Identification and Security

We use a number of IT systems in the course of our business activities. They all have in-built security protocols at both system and user levels to prevent inappropriate access and use of data.

These systems are cloud-based so they can be accessed from any location. This also provides in-built data back-up and multi-centre storage to protect against loss of data.

MFA (multi factor authorization) will be enabled on all user access for added security, by virtue of a code sent to a mobile device.

Our Operations Database, which contains all coaching client data and reports, is located in AWS hosting based in the UK. Our internal documents and data are stored on Azure hosting based in the UK. Our HR system, Breathe, is equally kept secure within the UK. Genius Within specific client data is stored on our internal data base.

Access to each system is limited to only those who have a need to access the specific information.

When users leave the Company, or no longer need access to the system, their account access will be blocked, and the account archived, as necessary.

Email and document file access be transferred to their line manager and O365 will purge the account 30 days after their removal from the system.

Also see the Company IT Systems list.

Customer Systems and Data – Authorised Use and Security

The confidentiality, integrity and availability of all customer information must be assured and therefore all employees will be trained and familiar with customer data handling requirements.

Any customer supplied technology, or access to their systems, will be managed in strict accordance with the customer supplied procedures. Where stipulated, all employees accessing customer supplied data and systems will be fully vetted, trained and have ongoing access to the relevant systems operating procedures that set out the appropriate use of customer IT.

Any breaches of customer procedures will be reported immediately to the Chief Operating Officer. They will inform the customer immediately using their defined reporting procedures. An Incident Report will be raised, the cause of the breach will be identified, and actions taken to ensure it doesn't occur again.

Data related to information logged on customer secure systems, will be referenced on our own internal systems by code, ensuring that no whole names (first and surname) of vulnerable adults are listed to ensure that anonymity is preserved. This might include receipts for discretional purchases, travel information etc.

Genius Within Technology Assets

As the Company stores information and conducts business via cloud-based IT systems, it is essential to protect the technology used to access those systems.The main threats to

our hardware are physical: loss, theft, or damage. Cyber-attacks, i.e., virus/malware attacks and hacking by exploiting system vulnerabilities are also a key threat.

No essential information is stored locally on any hard drive so the loss of hardware will have minimal effect on the business. However, it will need to be replaced and so care should be taken to prevent loss, theft, or damage.

Our Plumpton and Birmingham offices are locked every evening - including internal and external doors.

The Plumpton Racecourse site gates are locked every night, preventing unauthorised access to the site and laptop computers and portable devices, such as mobile phones, are locked away in a filing cabinet when not in use.

The Birmingham office is security manned with key card access only.

Obsolete hardware such as computers or external data storage will be securely wiped to remove any business information.

The Company maintains an Asset Register of all company purchased technology e.g., Laptops, mobile phones and anything over £100. The Register records the following information:

- device type
- brand and model
- serial number
- purchase date
- purchase value
- responsible person
- project associated – e.g., was this asset purchased as part of a specific project?

The hard drives from the Company's computers will be overwritten using an approved commercial overwriting product if they are to be reused or shredded if they will no longer be in use.

Also see the Asset Register.

Genius Within Data

All data created for the company, on behalf of the company or stored on company maintained systems is the property of the company. Company data cannot be stored on personal devices or sent to a personal email address, this includes sending emails from a personal email address. No employee, associate, customer, or client data is to be stored on a portable storage device such as a USB memory stick or external hard drive. It may only be accessed via the designated IT system and by authorised users.

Company data is inclusive of all data and communications (emails, teams, call logs) stored on company maintained platforms, devices and company paid subscriptions services (such as Office 365 and Zoom). And as such we maintain the right to look at any data stored as and when we deem necessary.

Using Personal Computing Devices for Work

Due to the geographical location of our associate network, our Operations Database and email systems are designed to allow associates to remotely access their client's data, prepare reports, and upload contact sheets.

As our email (Outlook) and information sharing systems (Operations Database and Share Point) are cloud based, it is also possible to access them on mobile devices such as smart phones and tablets.

Anyone accessing Company information must at all times give due consideration to the risks of using personal mobile devices. To access GW's Microsoft 365 (outlook, teams, sharepoint etc.) your mobile device must be enrolled with Microsoft Intune, have a 6 digit

Pin and screen lock of no longer than 10 minutes and on the latest Operating System. It will not be possible to access GW's Microsoft 365 without these in place.

Basic precautions as outlined in this policy must be followed and will be audited. These precautions are especially important where other users have access to the computer or device.

It is strictly prohibited to access customer systems from any computing device other than those provided or approved by the Company or the customer and designated for that use.

IT Disaster Recovery

The Company maintains a 'disaster recovery pack' for our two main systems:

website

database

These are maintained by external contractors, who are adequately insured, and includes all the necessary access codes and details to take over management of the system should the contractor's companies dissolve for any reason.

The risks to our IT systems are reviewed as part of our Business Continuity Plan.

Use of Email, Internet and Social Media

The Company utilises email systems as well as the internet and social media in the course of conducting business. Each employee and associate are given an email account, when they have completed the security checks, as part of their induction process and asked to reset their password.

This email address is to be used primarily to contact customers, clients and for internal use. Associates should not use their personal or own business email accounts to contact Genius Within clients or customers. In order to maintain our expected level of customer

service we will be completing monthly spot checks of all emails for quality checks, effective from March 2023.

Personal use of a Company email account should be kept to a minimum.

The Company internet and social media presence is administered by our Marketing Team. However, it is acknowledged that employees and associates will have their own personal accounts.

The following guidelines apply to all use of emails, internet and social media for communication about Genius Within and its business:

- Do not open or email attachments from an unknown source in case they contain a virus
- Do not respond directly to any phishing or spoofed emails
- Report any phishing or spoofed emails to the Finance Manager
- Do not visit websites that have inappropriate content
- Do not disable security or email scanning software
- Do not send sensitive or confidential company or client data via email
- Do not allow others to access your email or social media accounts
- Ensure passwords are strong, changed regularly and not shared with others
- Do not send emails or post messages that may be seen as defamatory, offensive, harassing or otherwise damaging or likely to incur liability for Genius Within
- Do not create or distribute any inappropriate content or material via email or social media
- Do not use emails or social media for any illegal or criminal activities

Whilst working with our clients and customers, we encourage our employees and associates to develop strong working relationships. However, professional boundaries should be maintained at all times and so personal friendships via social networking sites should not be pursued.

Where specified, customer provided email systems (e.g., the secure CJMS system)In these instances, accounts will be provided to relevant users only and should be used for all project and customer communication.

These systems should only be accessed via Genius Within or customer provided computers and not forwarded on to other accounts or devices.

Website Privacy and Cookies

Our website www.geniuswithin.org collects user information via cookies. This information is used solely for internal use, i.e., to measure traffic to a given page or for user access to our e-Learning modules (accessed via the website). No user data collected is sold or otherwise shared outside of Genius Within CIC, nor is it used to send mailshots or mass marketing campaigns.

Website users are informed of our use of cookies are and given the option to opt out of their use.

Protection Against Internet Based Threats

The threats posed by cyber-attacks can be minimised by following these rules:

- All passwords should be changed monthly, should be a minimum of 8 characters including a mix of upper- and lower-case letters and numbers or characters
- Applying a strong lock-screen password to each PC or device
- Do not auto-save passwords within an IT system or allow other programs to do so, e.g., Google Chrome or Microsoft Edge. Where we find, under The Equality Act 2010, an employee is identified as needing a reasonable adjustment, to perform their role, then we will apply individual review of this policy to accommodate their needs in balance with our management of risk.
- PCs and devices should automatically logout any user after 10 minutes of inactivity

- If a device is used by more than one person each should have their own password protected account
- Unused accounts should be deleted to prevent unauthorised access

Turning on the Firewall software and allowing only approved network traffic:

- MS Office
- SharePoint
- Core Networking
- Network discovery
- File and printer sharing
- Google Chrome
- Skype
- Zoom
- Teams

All other traffic should be prevented from passing the firewall and the user notified if unauthorised access is attempted.

Remote access software and firewall access should not be activated on any devices except in exceptional circumstances. This access should be pre-approved by the IT Manager and deactivated/deleted as soon as it is no longer required.

Ensure all software is kept up to date. Patches and updates are installed within five working days of issue. This will be carried out centrally.

Run Microsoft Security Essentials daily and ensure Real-time protection is turned on. This will be carried out centrally.

Clear cookies and internet history daily.

Ensure all email accounts have virus checking activated. This will be carried out centrally

Do not open any email attachments from unknown sources.

No software may be installed or downloaded on to a Company owned computer without pre-approval by the IT Manager.

Disable auto-run features on software.

Old, obsolete or unused software should be removed from the computer.

This policy should be read in conjunction with our Password Policy which sets out our requirements for secure password creation and management.

Linked/Relevant/Referenced Policies

GDPR Policy

Password Policy

Revision History

Revision	Changes	Author	Approver	Date
1A	New Document	S Scrase	Nancy Doyle	10 04 15
2A	Changes identified in review made, Operations Director renamed to Systems Director.	S Scrase	Nancy Doyle	02 07 16
3A	Changes identified in review made.	S Scrase	Nancy Doyle	22 10 16
4A	Change of reporting issues process and an addition of use of Google Drive	M Symons	Fiona Barrett	19 01 18
5A	Changes following review	M Symons	Fiona Barrett	14 05 19
6A	Review of policy	Dom Nally	Nancy Doyle	08 09 19
7A	Review of policy	H Charnock /D Nally	Fiona Barrett	2020 0902
8A	Review and change of operating systems	Fiona Barrett	Helen Charnock	2021 06 11
9A	Review and inclusion of Genius Within Data	Alex Preston	Helen Charnock	2023 02 15
10A	Review- updated clear desk and portable media	M Symons	F Barrett	2023 10 19

11A	Review and Updated phone policy	A Preston	F Barrett	2025 03 03
12A	Reviewed	H Charnock	F Barrett	2026 06 29