

Ginger Nut Training.



Document Title

Ginger Nut Training – IT Security Policy

Originator

Directors

Responsible Person

Directors

Date of Approval

August 2024

Policy Due for Renewal

August 2025

Version

10.1.0

ginger nut®

IT Security Policy

Purpose

As a training provider and data manager / processor we have access to significant quantities of data which should be managed and controlled in accordance with our Data Protection Policy.

In addition to this all staff have a responsibility to ensure that data that they can access remains secure and, as such, should follow this security policy at all times. Where you are provided with a computer/mobile phone or any other device to access company data you must comply with the Device Sign out form and all other appropriate policies.

Please note that your login details are YOUR responsibility. Complying with this policy at all times is a minimum expectation for all staff and failure to apply the rules below constitute a formal disciplinary matter with all disciplinary outcomes possible, including termination of contract.

Passwords

All passwords should:

- Be unique – do not re-use any passwords across any sites
- Be at least 8 characters long
- Contain at least 2 alphanumeric or special characters
- Should never be shared unless strictly necessary and never outside Ginger Nut Media

Where available we use multi-factor authentication any sites which hold personal or company data. Where this is done you are responsible for the security of the device that is used for authentication and for ensuring that only your login attempts are authorised.

Mobile Devices

Where a mobile device is used to access company data it must use a supported version of Android or iOS and be kept updated with all security patches.

Access to the device must require a minimum of 6-digit PIN and/or Biometric access.

Device Security

Without specific agreement you should never access company data on any device not owned but Ginger Nut Media Ltd – this includes personal computers and phones. If you need to access these files outside of a Ginger Nut device, you must have approval from a Director or senior manager.

For all devices that are used to access Ginger Nut Media's data or files you may be asked to comply with the following:

- Download company approved and supplied security software to allow us to monitor security
- Ensure tracking of devices and remote deletion of data is possible in case of loss or theft
- In some scenarios Ginger Nut Media may need to remotely delete data from your device – this would be limited (as far as practicable) to company owned data and would only be carried out where strictly necessary

Authenticator apps may be installed on personal devices if required but you are responsible for the security of the device and any access to your accounts.