Information Security Policy

a) Company Owned Devices

This part of the Policy relates to employees who have received a company owned device such as laptop/tablet/ mobile phone.

This policy is designed to ensure that our employees use strong security practices when connecting to the company network or accessing business emails, thus protecting the company from cyber threats, hacking and data breaches.

If you are using your company owned device and have access to a business email address, Gmail Authenticator and Sophos Authenticator will be downloaded onto your company owned phone if required. Authenticator Apps generate a one-time code that you use to confirm that it's you logging in to a website or service, this provides the second part of what's called two-factor authentication (2FA). Authenticator Apps can be used to protect applications such as social media and emails.

You are also required to install major software updates within 14 days of release on all devices. Software updates are important because they often include critical patches to security holes. They can also improve the stability of your software and remove outdated features. All updates are aimed at making the user experience better and more secure, and gives the peace of mind that you are on the most up to date operating system for your device.

You must let us know if your device is lost or stolen as data breaches could occur if untrusted parties retrieve any unsecured data present on the device.

You are not permitted to download any personal applications to your business device. This will be seen as a security breach and could reduce the security of the device.

All apps must be purchased via the app store, phones must not be jail broken and here is a list of approved applications;

- Microsoft Outlook
- Gmail
- Google Chrome
- Microsoft Office
- Adobe
- Zoom
- Microsoft Teams
- Google Authenticator
- Google Maps
- Sophos

Company software downloads can only be done by an administrator. Each device is set up with both user and administrator accounts, the 'administrator' account is only used when changes are required and is password protected which the 'user' does not have access to.
Members of staff who have been given 'admin' rights are trained and have signed an agreement to ensure that they will not use the account for general usage, i.e. accessing websites or emails.

On your company owned device you are only permitted to open your business emails in Gmail or Outlook, use google chrome and Own cloud.

Cloud based file storage applications outside of the company's own are not permitted i.e. Drop Box

USB sticks are not to be used or allowed in Company Equipment.

b) BYOD (bring your own device)

This part of the Policy allows employees to use their personally owned devices for work-related activities, rather than using a company owned device.

Fully supporting the use of personally owned devices in the workplace eliminates the need for employees to carry two phones. This BYOD policy is designed to ensure that our employees use strong security practices when connecting to the company network or accessing business emails, thus protecting the company from cyber threats, hacking and data breaches.

This policy is in particular reference to employees who have a business email and wish to use personally owned device at work.

If you are using your personally owned device for business purposes and have access to a business email address, you are required to download Gmail Authenticator. Authenticator Apps generate a one-time code that you use to confirm that it's you logging in to a website or service, this provides the second part of what's called two-factor authentication (2FA). Authenticator Apps can be used to protect applications such as social media and emails.

Access to the company server away from the office will require Sophos authenticator. You are required to download this to your personal device to gain access.

All apps must be purchased via the app store, phones must not be jail broken if you wish to use your personally owned device for work-related activities.

You are also required to install major software updates within 14 days of release. Software updates are important because they often include critical patches to security holes. They can also improve the stability of your software and remove outdated features. All updates are aimed at making the user experience better and more secure, and gives the peace of mind that you are on the most up to date operating system for your device.

If you are accessing business emails on a personally owned device you must let us know if your device is being replaced, lost or stolen as data breaches could occur if untrusted parties retrieve any unsecured data present on the phone.

If you sell your device you must wipe all sensitive information before handover.

..... Managing Director ..... Finance Director

Date: 15/04/2024 Date: 18/04/2024