CYBER PROTECTION POLICY

Company name: _____

Created: _____

Last updated: _____

Review date: _____

ENDPOINT SECURITY

The business must have up-to-date endpoint protection that includes:

- ☐ *Remote device management*
- ☐ *Malware detection*
- ☐ *Multi-layered protection*
- ☐ *Real-time notifications*
- ☐ *Cloud management*
- ☐ *Simple reporting*

_____ is responsible for purchasing and managing this database.

BRING-YOUR-OWN-DEVICE

All devices must have access authentication.

Staff must use _____ to generate and store strong passwords.

Where possible, staff should use two-factor authorisation to protect their devices.

Only devices used for work purposes should be connected to the network.

staff should use _____ for personal activities such as checking social media.

STAFF TRAINING

The following training module must be taken by all staff when they join the business:

DATA MOST AT RISK

WHO CAN ACCESS WHAT

Employees will only be given access to information they require to complete their job. If you no longer require access, you should raise this with your line manage so that your access can be revoked.

WHAT TO LOOK OUT FOR

Employees must report the following issues:

- *Unusually slow computer*
- *Difficulties logging in*
- *Internet connectivity problems*
- *Unexpected website redirects*
- *Suspicious-looking emails, links or attachments*

CLOUD SECURITY

Staff will only be given access to information that they need to complete their work. A record of which employees has access to what data will be stored here:

When a staff member leaves, their email account will be deactivated and access to business information and files will be revoked.

This must happen within Following this, all passwords will be updated within

DATA COMPLIANCE

We must comply with the following data protection regulations:

Where necessary, training budget will be granted to ensure this person has the relevant skills and knowledge to carry out this role.

Staff must refer to

regarding any issues related to data compliance prior to taking action.

Internal data compliance audits will take place once every

Where data is not kept in accordance with the relevant data compliance, actions will be taken within the following

to rectify this.

ADDITIONAL NOTES

SAVE PRINT