moreton
&PARTNERS

Information Security Policy

It is the established policy of Moreton & Partners Limited to operate within the requirements of a documented Information Security Policy to comply with all statutory, regulatory and contractual requirements, and to protect the interests, property and information of the company, and of its clients and employees, against cyber threats or loss.

The purpose of this document is to set out the Company's IT security requirements to ensure that appropriate measures are in place for the secure management our IT systems, equipment and devices thus giving Clients and staff confidence in our ability to protect the information we hold.

The aim of the policy is to:

- Reduce the risk of IT problems
- Enable continuity of service provision should something does go wrong
- Protect company, client and employee data
- Keep valuable company information secure
- Meet our legal obligations under the General Data Protection Regulation and other laws/regulations
- Meet our professional obligations towards our clients and suppliers
- Provide an environment where the risk of loss or damage is minimised and managed
- Minimise the company's liability for lost or damaged property
- Ensure incidents of loss or damage are dealt with swiftly and effectively
- Ensure the process is administered with our quality management framework

Responsibilities of all users:

Effective security is a team effort requiring the participation and support of every member of the Practice. It is the responsibility of all staff to know and follow these guidelines as everyone is personally responsible for the secure handling of confidential information entrusted to them. Employees may access, use, or share confidential information only to an authorised and necessary extent for the proper performance of their duties, in accordance with Company policies, legislation and regulations.

All users must:

- Promptly report any theft, loss or unauthorised disclosure of protected information, IT equipment or any breach of this policy to Marie Moreton, Data Controller.
- Exercise care to protect and safeguard all IT property under the individual's control.
- Do not use removable data devices to transport information. The company's 365 SharePoint accounts are in place to avoid the need and security risk of using such devices to negate the potential risks.
- Remove software that is not used or needed from your IT equipment
- Update operating systems and applications regularly
- Store files in official Company storage locations
- Understand the privacy and security settings on phones and social media accounts
- Ensure computers and phones log out automatically after 15 minutes and requires a password to log back in
- Not share company IT equipment.
- Report to the Marie Moreton, Data Controller, if property is incorrectly used, lost, damaged, or otherwise found to be unsuitable for use.

Host Employers

With regard to employees who are based at Host Employers (Client) offices using the Host Employers IT systems and devices, please ensure that you are aware of and adhere to the Host Employers IT security and password protection policies and requirements. If you are unaware of requirements or require clarification on any of the conditions, please contact your line manager or the Practice Manager to enable your queries to be addressed and resolved without delay.

Working from home

As part of our IT security policy requirements, it will be necessary to ensure that the default pre-configured password on your home router has been changed in accordance with the password requirements detailed above (password creation). For example, the password that is provided with a home hub (BT, Virgin, Sky etc.) must be changed from the default password to a password of your choice. This must be done to ensure the integrity and security of our systems and data.

Be alert to the security risks

While technology can prevent many security incidents, your actions and habits are also important. With this in mind:

- Take time to learn about IT security and keep yourself informed. www.gov.uk/government/collections/cyber-security-guidance-for-business is a good source for IT security awareness.
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender. If you have any doubts about the safety of the attachment, delete the email permanently from your device. Do not attempt to open suspect attachments.
- Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee, client or company confidential information. Fraudsters and hackers can be extremely persuasive and manipulative.
- Be wary of fake websites and phishing emails. Do not click on links in emails or social media.
- Do not disclose passwords (as detailed within the Company's IT Security – Password policy) and other confidential information.
- Use social media in a professional and responsible way, without violating company guidelines or disclosing confidential information.
- Take particular care of your computer and mobile devices when you are away from home or out of the office.
- If you leave the company, you will return any company property, transfer any company work-related files back to the company and delete all confidential information from your systems as soon as is practicable.
- Where confidential information is stored on paper, it should be kept in a locked secure place where unauthorised people cannot see it and shredded when no longer required.

Senior Management Team (SMT) Responsibilities:

- The SMT must comply with the requirements stated above.
- It is the responsibility of the SMT to ensure that the Company's IT systems are as secure as possible.
- The SMT must ensure that all security measures must be kept up to date in line with current requirements and industry best practice.
- To ensure that all data is stored securely which is performed and controlled by our IT Support company and continues to be secure and adequate for purpose.
- The SMT must continue with implementing Cyber Essentials certification and to ensure that the required QM annual audits are undertaken promptly.

- Devices and equipment that is no longer in use must be disposed of and destroyed by our quality managed IT providers. A certificate of disposal must be obtained to ensure that no data risk is possible.
- To consider the following IT security measures and discuss implementation with our IT Support company to ensure suitable protection is in place:

  - Boundary firewalls
  - Internet Gateways
  - Secure configurations
  - Access control
  - Administration account management
  - Malware Protection
  - Patch Management
  - Password based authentication
  - MFA
  - Anti-malware software
  - Whitelisting
  - Sandboxing

Prohibited actions

The following matters (among others) are prohibited on Company systems and while carrying out your duties for the Company. Non-compliance may result in disciplinary action:

- Anything that contradicts our equality and diversity policy, including harassment.
- Inappropriate internet/email usage (please see the Company's 'Email, Internet and Social Media Usage Policy and Guidelines' document)
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of confidential information at any time.

Please bear in mind that devices connected to the internet can possess the possibility of quickly being afflicted with spyware programs and a variety of viruses. These malicious programs can result in data corruption or worse, with the Company's data being made available to unauthorised parties as the result of the infection. It is therefore imperative that all employees, sub-consultants, temporary staff and the SMT exercise care to protect and safeguard IT systems and equipment under their individual control. All equipment, laptops and mobile phones, must be stored securely especially when taken offsite. Any specific requirements of Host Employers must be adhered to as stated within our Third Party Property Policy. Failure to secure IT equipment in the required way could result in disciplinary procedures.

This Information Security Policy, which is not intended as a stand-alone document, is supported by related Company policies and procedures and the Quality Management System (QMS), which defines our Company's activities.

This Information Security Policy is maintained by audit and review, and by the methods described in the QMS, in order to provide effective assurance that all aspects of company, employee and Client specified security requirements are being implemented.

Director in Charge ……………………………………Matthew Moreton

Practice Manager ……………………………………Marie Moreton

Date: 29th April 2025

V8.0
29th April 2025