IT Security / GDPR / Privacy Policy

This Policy helps us reduce the risk of IT problems, plan for problems and deal with them when they happen, protect company, client and employee data, keep valuable company information, such as plans and designs, secret, meet our legal obligations under the General Data Protection Regulation and other laws and meet our professional obligations towards our clients and customers

Responsibilities

- Austin Ambrose is the director with overall responsibility for IT security strategy.
- Sue Chadwick has day-to-day operational responsibility for implementing this policy.
- Pete Mylett of CPM Computers is the IT partner organisation we use to help with our planning and support.

Information classification

We will only classify information which is necessary for the completion of our duties. We will also limit access to personal data to only those that need it for processing. We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources appropriately:

- Unclassified - this is information that can be made public without any implications for the company, such as information that is already in the public domain.
- Employee confidential - this includes information such as medical records, pay and so on.
- Company confidential - such as contracts, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.
- Client & Learner confidential - this includes personally identifiable information such as name or address, passwords to client systems, qualifications, client business plans, new product information, market sensitive information etc.

The deliberate or accidental disclosure of any confidential information has the potential to harm the business. This policy is designed to minimise that risk.

We do not protectively mark documents and systems. Therefore, you should assume information is confidential unless you are sure it is not and act accordingly.

Under the GDPR, where a data breach is likely to result in a 'risk for the rights and freedoms of individuals' we must notify the customers and data controllers 'without undue delay'. We will ensure we inform them within 72 hours.

Access controls

Internally, as far as possible, we operate on a 'need to share' rather than a 'need to know' basis with respect to company confidential information. This means that our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

As for client / learner information, we operate in compliance with the GDPR 'Right to Access'. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose. Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format.

To protect confidential information, we have a robust recruitment and induction process that includes the creation of a user account and the required access privileges for the specified user.

When someone leaves all of their respective user accounts are immediately disabled.

Admin privileges to company systems will be restricted to specific, authorised individuals for the proper performance of their duties and this is signed off at Director level.

To protect our data, systems, users and customers all our equipment is installed with anti-malware software which is set to update daily and scan files automatically upon access.

When a new employee joins the company, we will add them to the company Office365 system, creating an email account and granting appropriate access to the SharePoint structure as necessary pertaining to their role. In addition, if appropriate they will be granted access to our Aptem system.

PMA Team responsibilities

Effective security is a team effort requiring the participation and support of every employee and associate. It is your responsibility to know and follow these guidelines.

You are personally responsible for the secure handling of confidential information that is entrusted to you. You may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to Austin Ambrose.

It is also your responsibility to use your devices (computer, phone, tablet etc.) in a secure way. At a minimum:

- Remove software that you do not use or need from your computer
- Update your operating system and applications regularly
- Keep your computer firewall switched on
- For Windows users, make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date. For Mac users, consider getting anti-malware software.
- Store files in official company storage locations so that it is backed up properly and available in an emergency.
- Understand the privacy and security settings on your phone and social media accounts
- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers.
- Don’t use an administrator account on your computer for everyday use
- Don’t share your password with other people or disclose it to anyone else
- Don’t write down PINs and passwords next to computers and phones
- Be alert to other 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.
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender.
- 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. Don’t click on links in emails or social media. Don’t disclose passwords and other confidential information unless you are sure you are on

a legitimate website.
- Use social media, including personal blogs, in a professional and responsible way, without violating company policies 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 secure place where unauthorised people cannot see it and shredded when no longer required.

The following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:
- Anything that contradicts our equality and diversity policy, including harassment.
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of confidential information at any time.

Main Contacts:

Name	Job Title	Address	Mobile phone
Ian Jones	Operations Director	ian@practicemanagersuk.org	07880 788 985
Austin Ambrose	Client Services Director	austin@practicemanagersuk.org	07726 921 685
Lisa Lindgren	Head of Education	lisa@practicemanagersuk.org	07751 091 395

Should you have any concerns around Safeguarding please email:

PMA DSL, Lisa Lindgren at: safeguarding@practicemanagersuk.org

Please be assured your email will be treated in the strictest confidence and that you will receive a direct reply from Lisa within 24 hours.

Revisions control:

Date	Summary of changes made	Changes made by (Name)	Version No.
17th Nov 2020	Creation of new policy to supercede Website & Privacy Policy, GDPR Policy and GDPR statement	Sue Chadwick	V1.0

Next Review Due: August 2021