Information Security Policy for The Markland Clinic

Your Responsibilities

All clinical and non clinical staff who process information assets from and for The Markland Clinic are accountable for Compliance with this Policy. When using information, any accidental breach of this Policy must be reported to the Manager as soon as you become aware of it. Transmission of information must be via a secure electronic method.

As part of our information security requirements you must ensure that:

- You comply with all requirements of any contract between you and The Markland Clinic.
- You adhere to the principles and directives in this Policy at all times.
- All possible software updates are downloaded an installed to increase security on mobile devices.
- All devices used to hold or connected to devices that hold The Markland Clinic
- information are password controlled. Passwords should contain at least 1 capital letter, 1 number and a special characterand be a minimum of 8 characters long.
- Anti-virus and malware protection is used where available to protect any devices which store The Markland Clinic data.
- A client's identification is checked when conducting examinations or tests.
- The caller's identity is verified before divulging any information on the telephone.
- All breaches are reported to a manager.
- All medical reports, results/documentation are sent via a secure method.
- You adhere to data protection requirements in accordance with recommendations or requirements of the ICO and your professional body.

Data Integrity and Availability

Staff who use laptops and/or hand-held mobile devices are responsible for ensuring the integrity of the data they process. Data must be backed up on a regular basis to ensure data integrity and availability.

All laptops and/or hand-held mobile devices used by the examiners for business purposes must be maintained with due diligence. Sufficient controls need to be taken to ensure that the equipment is secured at all times.

Laptops and/or hand-held devices must not be left in cars unattended for any periods of time.

Laptops and/or hand-held mobile devices and other mobile devices must not be left unattended under any circumstances when they are used in teleworking or public locations.

1.1 Netwok Access

Access to The Markland Clinic supplied software must only be made from password protected devices. Passwords should contain at least 1 capital letter, 1 number and 1 special character and must be a minimum of 8 characters long.

The minimum acceptable level of security for connection to a WIFI network is WPA or WPA 2 (Wired Equivalent Protection/WEP is not acceptable standard). Laptops and other mobile devices must not in any circumstances be connected to an unsecure WiFi network (whether via a public wireless access point, wireless 'hotspot' or otherwise).

1.2 Anti-Virus and Malware Protection

Staff using any device are required to ensure that anti-virus and malware protection controls are installed and regularly updated on the local machine. It is the responsibilty of staff to report problems with virus or malware protection controls to the appropriate manager.

Under no circumstances should the operation of any anti-malware software of firewall be disabled and it is vital that any laptop or handheld mobile device has appropriate security measures.

1.3 Security Breaches, Hacking and Lost Equipment

It is the examiner's responsibility to ensure that any suspected breach of security by accident or deliberate intrusive action by another (such as hacking) is immediately reported to the appropriate manager. If any equipment that holds The Markland Clinic clients details is lost, this must also be reported immediately.

Failure to report any breach as detailed above will result in suspension of instructions and possibly reporting to the ICO.

1.4 Telehone Handling

On a call, examiners must always ask appropriate Data Protection questions before passing on any information relating to a Markland Clinic client.

1.5 Destruction of Media

Not later than 6 months (or agreed timescales) following the completion of the request, all information linked to The Markland Clinic that is no longer required to complete the service for which examiner has been engaged must be permanently deleted from any laptop or hand-held mobile device on which it is stored and any physical copy must be destroyed. Physical paper copies must be destroyed by confidential shredding.

1.6 Information Transfer

All staff should use Outlook as their secure email provider. Unsecure webmail providers such as Hotmail, Yahoo, Outlook.com etc are not appropriate vehicles for transfer of sensitive information. Attachments sent by email must be password-protected and he password must be sent by separate email.

Medical reports should not be sent by post. If this is the only option available then the report must be sent by trackable post and a copy retained. This copy should then be securely destroyed witin our agreed timescales (not usually more than 6 months).

Facsimile machines are not secure and The Markland Clinic actively discourages their use.

1.7 Physical Media Transfer

All examiners should only send physical media through trackable postal services via couriers. Examiners should only send physical media in packaging that is sufficient to protect the contents. Physical media such as CD's should be encrypted and the encryption should be sent under separate cover.

1.8 Sharing of Information with Supply Chain

Staff of The Markland Clinic must ensure any information in any form provided to their own suppliers of subcontractors is protected using the same principles discussed in this document and that the Data Protection Act is adhered too.

The Markland Clinic should also be consulted if any of the suppliers that are used are working outside of the EU and in what capacity. The Marland Clinic discourages the passing of data to any other subcontractor outside the EU.

1.9 Protection of Records

It is the examiners duty to keep all physical or data records secure when not in use. Data records should be kept in a secure file, not on a desk top. Physical records should always be kept in a secure locked cabinet when not in use and never left in a public space.

All cryptography for that data should be kept securely and separately and kept for as long as the records themselves.

The examiner should store the records in a format or location that enables the examiner to be able to access it without complication and return it to The Markland Clinic if required.

