LEAD
ASD Diagnosis

DATA STORAGE POLICY

Document Detail	
Effective from	8/2/19
Reviewed	28/06/2023
Date of next review	July 2024
Document version	V1.3
Owner	LEAD Manager

Personal Data includes information relating to a person/s who

- **can be identified or who are identifiable, directly from the information in question; or**
- **who can be indirectly identified from that information in combination with other information.**

This information is confidential and may include details of name, address, details of condition, test results, staff records etc.

Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. If personal data can be truly anonymised then the anonymised data is not subject to the requirements of GDPR .

All confidential data should be stored and processed securely. This is especially important in the case of patient data, or other data identifying individuals such as staff, visitors, and contractors, and also of sensitive financial and business data.

It is the responsibility of all staff to ensure that confidential data is properly secured at all times, whether on PCs, laptops, being emailed, or placed on removable memory devices, etc.

Remote access generally carries a higher risk of unauthorised access to information due to lesser degree of control over local conditions of the remote session.

All data on laptops, desktops, and portable data storage devices that contain information about an individual or their health must be encrypted

USE OF LAPTOPS

- Use strong but memorable passwords, these should be easy to remember and difficult to guess.
- It is also a good idea not to use words such as your child's name, pet's name, or your favourite sports team. This type of information might be easily viewed on your social media page e.g. Facebook, Instagram, Twitter etc. Numbers and symbols can still be used but it is national advice to use three random words as the key to creating a strong password.
- Use a strong, separate password for your email and other important accounts. This means if criminals steal your password for one of your less important accounts, they cannot use it to access your most important ones. This includes your main email account. Criminals can

potentially use your email to access many of your personal accounts and find out personal information. If this is your bank details, address, or date of birth, you might be left vulnerable to identity theft or fraud.

- For your most important accounts, if it's available, you should use Two-Factor Authentication. This means involving a second step after entering your password e.g. providing a fingerprint, using Eye/Face identification, answering a security question, or entering a unique code sent to your device.
- Logout of the session when you have finished working
- Keep the passwords secure; If you need to write down a password, make sure these are kept in a secure location that only you have access to (e.g. locked cabinet)
- Do not leave the workstation unattended while you are logged in, even for a short time, without taking appropriate measures to secure it, at the workplace or at home
- Always place work documents into an encrypted volume on a Laptop. Any confidential data should always be encrypted.

<u>Physical security</u>

• Ensure the laptop is physically secure whether at work or home - hidden out of sight or locked in a cabinet overnight, for example.

• Ensure that laptops are out of sight when travelling with them by car.

<u>User login</u>

• Ensure ALL Accounts have 'strong' passwords on them.

• Ensure a limited number (eg "Administrator" only if possible) have "admin" rights.

<u>Data on the Laptop</u>

• Ensure there is no confidential data on the "open part" of the C:\ drive – keeping it on your "desktop" / 'My Documents' is more secure.

• To be properly secure against a real ‘attack’ on the laptop, create an encrypted volume on the C:\ drive. ALL confidential data must go into this area on any laptop, including partially anonymised data. “Strong” passwords are a must.

• Ensure latest versions of antivirus software is installed.

USE OF REMOVABLE MEDIA

- Personal data and other sensitive information must be encrypted when stored on removable media.
- Where removable media devices are to be reused then any stored data or information must be securely erased before reuse or the device destroyed.
- Only store data on USB memory devices if it is necessary, and delete it when it is no longer needed
- Store USB devices securely when not in use
- Take precautions to protect the device from damage, loss or theft
- If a device containing confidential or personal information is lost or stolen, you MUST immediately report this.
- Use an encrypted Flash Drive

EMAILS

- Send emails across secured connection on Internet (https://), or as encrypted attachment.

Emailing patients

If communicating with patients by email it is acceptable to send parents confidential information about their child's diagnosis after their consent to use email has been obtained and documented, and their email address has been verified.

If sending an email to a third party / collaborator

attachments to emails that contain confidential data must be encrypted

If you use email client software such as Outlook Anywhere on a personal device to access work email, you must make sure that your device is configured securely (e.g. encrypted and uses a PIN/password to access the device). You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

Do not put person identifiable data (PID) in the subject line of emails (such as patient name/number etc.)

USE OF HOME COMPUTER FOR WORK

If you use a Home computer to work on, ensure it is physically secure at all and data is physically secure (encrypted).

- Use encryption to create a volume on your own PC for work documents to be held, if they are of a confidential nature.

- Physical security of your PC or laptop is more of a risk at home – ensure you keep your equipment safe in the house.

- Use NHSMAIL, as it uses a secure connection

- Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data.

- If using a PC, in a public area ensure the PUBLIC option is selected, so no trace is left of your user ID after logging out.

- Hotmail, Yahoo, etc. are secured connections, but a copy of sent mails, etc. will remain off-site (on their mail servers) unless you delete them. Also, the tendency is to use these accounts for home purposes, and there is more chance of being more 'lax' with strength of passwords, etc.

- If a regular user of NHSMAIL, please ensure you use a strong password, as this is all the authentication required to get into your Mail Account from anywhere in the world.

- If using a home PC, ensure Virus checking software is up to date

- Ensure data patches for your Virus checker are up to date.

- Ensure that your firewall is switched on and configured.

- Switch on Automatic Updates from Microsoft, which are invariably security patches.

WORKING WITH WIRELESS CONNECTIONS

• Secure your wireless router by ensuring that the administration password is switched on, with a strong password.

• Don't broadcast your SSID (your wireless network's name) – this will make your network visible to anyone nearby with wireless technology.

• You should always secure your wireless connection. It's better to use WPA / WPA2 encryption.

• Again, make sure the password for the above is strong.

PHYSICAL RECORDS

Physical records should be stored securely within a fixed lockable cabinet. The areas where equipment and physical records are kept should be secured appropriately.

All users of LEAD's information systems should understand their responsibilities to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Any suspected misuse of accounts or security incidents, such as loss of sensitive information or unauthorised access to personal information, must be reported to the manager