Information Security Policy

September 2018

This policy provides key principles to use digital tools provided by the trust securely. You must apply relevant safeguards to protect confidential personal data you handle at work. For the full version of this policy, click here.

Digital services

South London and Maudsley NHS
NHS Foundation Trust

Password security

A poorly chosen password may result in a compromise of the entire network.

The trust is implementing a new **passphrase policy** in line with the National Cyber Security Centre guidance:

- Be a minimum **length of 18 characters**
- Only need to be **changed every 90 days** (4 times a year)
- Optional to use alphanumeric (mixture of letters and numbers), or a mixture of upper and lower case characters
- Do not use passphrases that will be easy to guess, or passwords you use for other online accounts, such as social media
- Do not choose a passphrase identical or similar to the User ID or a passphrase identical to the previous 8 passwords
- **Never write it down nor share** in the clear or plain text
- If you suspect others know your password, change it immediately!

Physical security

Avoid paperwork duplication: Don't print emails, ePJS records. Printed copies are easily lost. Use secure mobile devices, such as trust provided tablets, smartphones instead.

Dispose of securely: If you have to print, shred securely as soon as the print-out has been used.

Be streetwise: If you need to carry confidential information, be cautious on public transport. Do not carry confidential documents unless all patient identifiers have been removed.

Housekeeping: Keep your workstations clear and paper-free. Tidy up confidential documents, dispose of securely, do not keep copies unnecessarily.

Office security: Follow the building and site security rules at work and do not allow unauthorised people unvetted access to areas that are not for public use.

E-mail security

@slam.nhs.uk is secure: Security of the email system is independently reviewed to ensure the controls are updated regularly against developing cyber threats.

Data Loss Prevention (DLP): An additional safeguard, the Data Loss Prevention (DLP), has been implemented to the SLaM email system which will automatically encrypt any emails that has personal identifiable information. You may receive an email if this is applied to email you send, but be assured, the email will be sent to your recipient in its entirety.

Always check that you are sending information to the correct recipient

Share documents rather than sending as attachments: Your documents on OneDrive are stored securely. You can share them directly from OneDrive with individuals of your choice. This is a great way to collaborate on the same document with colleagues.

Phishing and other cyber threats: Be mindful of suspicious emails and online scams designed to capture your personal details, such as passwords, financial information. Follow alerts and guidance from SLaM Digital Services. Improve your awareness.

Seek advice and support: Only use online resources provided by SLaM Digital Services such as tested Office 365 tools (e.g. OneDrive, Teams, Yammer etc.). Keep personal apps and tools for personal use. When in doubt, seek support from SLaM Digital Services.

If something goes wrong

For advice on privacy and data security:
informationgovernance@slam.nhs.uk

For phishing and email scams:
addspam@slam.nhs.uk

For technical queries and problems:
DigitalServices@slam.nhs.uk

Online security

Remember common sense: Protect your identity online. Only visit sites you know, learn about privacy settings and apply them. And remember, if something is too good to be true, it generally is…

Beware of social engineering tactics: Cyber criminals try to gather your personal information from your information that is already online often posted by you. Do not disclose personal data unless you are sure it is secure and relevant.

Use secure payment options if you shop online: Paypal and Apple Pay are options designed to avoid you entering your financial details on online shopping sites.

Device security

Switch on privacy and security features: All smartphones and tablets have features to lock with a pin, track if misplaced or wipe remotely if lost. Find out and turn these on.

Your security first: Do not display smart phones, tablets and laptops in public places making yourself a target for street crime. Be streetwise and protect yourself first.

Apps: If you are implementing new digital apps, contact IG for help with risk and privacy impact assessments at planning stages as early as possible.

Useful Yammer! Groups for more information

- FAQs and How to Guides
- O 356 Training
- Information Governance