

What You Should NEVER Do

- Do not create a password that is easy to guess, avoid personal information such as car registrations, names of people or pets, hobbies or interests.
- Write your password down and stick it to your computer or desk.
- Use the same password for all systems and applications.
- Do not share passwords or system accounts. To do so would contravene the seventh principle of the Data Protection Act. If a person needs access to something they do not have their own account for, they must speak to their manager to get access.

Further Information and Contact Details:

Service Desk

Wembley Centre for Health and Care
116 Chaplin Road,
Wembley,
Middlesex
HA0 4UZ

Phone: 020 8795 6676
Fax: 020 8795 6679
E-mail: servicedesk@brentpct.nhs.uk

Caldicott Guardian

Jim Connelly,
Director of Public Health and Regeneration
E-mail: jim.connelly@brentpct.nhs.uk

Information Governance and Data Protection Officer

Philip Maddocks
E-mail: philip.maddocks@brentpct.nhs.uk
Tel: 020 8795 7965

Password Management



Password Security

Your password is your main protection against someone else using your account and acts as a barrier against someone else accessing unauthorised information.

Passwords are the keys that open electronic doors and should be treated with as much care as a bunch of physical keys.

No matter how much money is spent on sophisticated network technology to prevent unauthorised access to data, a weak or poorly concealed password has the potential to bypass it all.

Remember that all activity on your account is deemed to have been made by you and unauthorised access is a criminal offence.

There should be no reason for you to have to share your password with anyone else, even for absence cover. However, if you have told someone your password for any reason, you should make sure that you change it again as soon as possible.

Follow the advice here and help us to keep patient and staff data secure and protected from unauthorised access.

Password Complexity

Your system password will need to be at least 10 characters long and must contain characters from 3 out of 4 of the following:

- Uppercase alphabet characters (A–Z)
- Lowercase alphabet characters (a–z)
- Numbers (0–9)
- Non alphanumeric characters e.g. \$ # , %

How Can I Remember A Complex Password?

A simple way to remember a longer and more secure password is by thinking of an original or catchy phrase such as; **“I always brush my teeth 2 times a day after meals”**

This would give a password of **“labmt2tadam”**

This uses Upper/Lower Case plus a number

Or

“why is it that Mondays always seem 2# as long!”

This would give a password of **“wiitMas2#a!”**

This uses Upper/Lower Case plus two Non alphanumeric characters.

What You Should Do

- Change your password regularly.
- Use a strong password.
- Choose a password that cannot be easily guessed.
- Always keep passwords secret.
- Change your password immediately if you suspect someone knows it.
- Log out or lock the computer when it is unattended.
- Try to use phrases to help make a complex and more secure password.
- Make sure nobody is watching you type your password.
- Report any suspected breaches of security to IT Service Desk.