NHS
East of England
Ambulance Service
NHS Trust

Working from home can bring freedom and flexibility – but it can also come with its own challenges. If you're working from home, here is some guidance to help you remain compliant with data protection laws.

Working from home – Data Security checklist

We understand that many of you have had to shift to homeworking very rapidly during the pandemic and that many will wish to continue with hybrid working – Our data security checklist will give you an initial overview and help you identify any security vulnerabilities.

General principles

☐ We have clear policies, procedures and guidance for staff who are remote working. These include topics such as accessing, handling and disposing of personal data. These can be found in the EEAST document library

☐ We are using the most up-to-date versions of remote access solutions.

☐ Where possible data should not be transferred from computer to paper copies.

☐ If paper copies are required then it would be advisable if they stay within the Trust premises (this may not always be feasible).

☐ Our staff use and understand the need for unique passphrases.

☐ We as users understand that it is critical to ensure that our user accounts are not compromised, by our usernames and passphrases becoming known by others.

☐ Multi-factor authentication (MFA) is available and can be initiated by contacting it support. MFA is recognised as a major defence against account compromise. This is why it is used by banks and financial institutes.

Remote applications

Remote application solutions such as Office 365 give staff access to the applications they need whilst working from home. This is to prevent staff from using their own personal applications to process personal data.

As we have move to hybrid working EEAST are developing long-term strategies and solutions to meet the needs of those working from home. We are using industry best practices and guidance coupled with the best software applications available.

Emails

As more staff will be working in the hybrid environment there will inevitably be an increase in email as a method of communication.

☐ We have reviewed and implemented the NCSC guidance on defending against phishing attacks. EEAST will regularly be disseminating information on phishing through a variety of methods. The new MetaCompliance is available to all users and contains all of the cyber security awareness training and can be accessed through EAST 24 Quick links or here.

☐ We have either blocked the ability to add forwarding rules to external email addresses or have a method in place to detect forwarding rules.

☐ EEAST staff should be aware of the need to use Trust email solutions and never use their own email or messaging accounts for the storage or transmission of personal/patient data.

How do I work from home securely? Ten tips

There can be a number of challenges to working from home. The IG Team have put together ten top tips to make sure data protection isn't one of them.

1. Follow EEASTs policies, procedures and guidance

EEAST have developed a robust approach to ensure that data is adequately protected. The Trust has invested significantly in providing applications and communication solutions to provide the right tools for the task. The temptation to do things in a way you think is more convenient, such as sending emails through your personal account or using the video conferencing app that you use with friends for work calls can lead to serious breaches of the Data Protection Act 2018 (DPA).

2. Only use approved technology for handling personal data

EEAST has provided you with technology such as hardware and software you must use it. These applications have been checked against a range of criteria, such as:

- Where is the data being held (the UK, the EEA or another country), not all countries have robust data protection laws?
- Is the data encrypted, at rest, whilst in transit? Failure to encrypt this data could end with personal data being intercepted.
- Who is responsible for each element of the data lifecycle?
- How will the data be destroyed when it is no longer needed (just deleting data is not sufficient)?

- If a data incident or breach occurs, who is responsible for reporting this to the Information Commissioners Office (ICO). Who will be informing the data subject (those who's data has been breached)?

- Who is the Data Controller (this is a term defined in the DPA) and who is the Data Processor?

3. Consider confidentiality when holding conversations or using a screen

You may be sharing your home working space with other family members or friends. Try to hold conversations, where they are less likely to overhear you and position your screen where it is less likely to be overseen. Consider if you monitor requires a privacy filter:

What is a privacy filter for a monitor?

A privacy filter is a thin piece of plastic that's placed over your monitor or display panel in order to prevent bystanders from absorbing confidential information.

4. Take care with paper and think before you print!

At the office, if you want to dispose of paper that contains confidential information you can use the blue confidential waste bins. At home you won't have that facility. The easy option is to reduce the amount of paper we use and to keep the information in its electronic format. Immersive readers (adobe and Word, both have this as an option) can make reading on screen easier.

If you do need to have a paper version, then you will need to ensure that is stored safely and securely until you are able to take them back into the office and dispose of them appropriately.

5. Don't mix Trust data with your own personal data

If you use a Trust device such as a laptop to undertake domestic activities, you must ensure that your domestic information is kept separate from EEASTs information and data to avoid accidental disclosure, deletion or alteration.

6. **Be extra vigilant about opening web links and attachments in emails or other messages**

Don't click on unfamiliar web links or attachments claiming to give you important updates or suggesting a degree of urgency. We're seeing a rise in phishing attacks so follow the guidance that has been provided. Both the IM&T team and the IG Team can provide more advice on what to look for in a phishing attempt.

7. **Don't panic if you do click on something or have entered details of your username and password after clicking a suspect link.**

The first thing to do is push Ctrl-Alt-delete and then select change password.
Once you have done this raise a support ticket with IT Support
Forward the suspect email to the Phishing@eastamb.nhs.uk address.
Contact the IG Team who will provide further assistance

8. **Use strong passwords**

EEAST have adopted the use of passphrases for authenticating accounts. But there are many applications that you use that will have a separate password requirement (both at work and in the domestic setting). It is recommended that you always use the longest password/phrase as the application will allow. 15 characters or above is very secure, using three random words such coffeetrainfish (15 characters) can be made exponentially more secure by adding 2 spaces, coffee train fish (17 characters), making the first letter of each word a capital even stronger.

If you are able to activate multi factor authentication then this will increase the security of your authentication.

9. **Communicate securely**

Use the communication facilities provided to you by EEAST. If you need to share data with others, then choose a secure methodology that is approved by the Trust. Filesharing applications like dropbox do not need

to be used as Microsoft Teams provides the ability to share files and folders both internally and externally in a safe way.

If you have to use email, which isn't always secure, consider password protecting documents and sharing the passwords via a different channel, like text message.

10. Keep software up to date

If you have Trust equipment then it will need to be a switched on and connected to EEASTs network so that the required updates and security patches can be installed on the device. If you have a Trust provided mobile phone, then please check that it is using the latest version of its operating system.

Hackers look for outdated applications (applications not using the latest version), as they have found the vulnerabilities that allow them to exploit the device, potentially letting them inside out network.