South East Coast Ambulance Service NHS
NHS Foundation Trust

Guidance for access to Office 365 on non-Trust devices

Version 2
October 2018
IT/IG

Introduction

South East Coast Ambulance Service NHS Foundation Trust (the Trust) relies on high quality information to underpin the delivery of high quality evidence-based healthcare and many other key service deliverables.

An effective information security and risk management regime ensures that the Trust's information assets are properly protected, reliable and available when needed.

Information has the greatest value when it is accurate, up to date and readily accessible where and when it is needed.

Current Position

This guidance document has now been reviewed 6 months after the initial implementation and in line with the new General Data Protection Regulation / Data Protection Act 2018 both of which became legislation on the 25 May 2018.

For the purposes of this document, the definition of 'non-Trust' relates to all forms of devices and services not owned or managed by the Trust. This include smartphones, tablets, desktops, laptops, terminals and home automation devices and services.

2. Background

Historically staff were able to view emails and attachments on non-Trust devices using Outlook Web Access (OWA). This option became no longer available following the migration to Office 365 which commenced during June 2017.

Following this migration the Trust Executive Team reviewed and took the decision in December 2017 to allow access to all Office 365 services from *any non-Trust or Trust owned device from any location which needs to be connected to the internet.*

The existing restrictions in Office 365 were then removed and the Trust implemented 'open access'. However, the permissions already present within SharePoint still remained, these permissions limit access and exposure to any sensitive documents to identified staff.

An initial guidance document was issued during December 2017 to support this change.

3. System access

This change allows staff to login to their Office 365 account from any location on any device, which needs to be connected to the internet. This access must be used responsibly and one of the key aspects to highlight is the access and use of email.

Access to email:
Under 'open access' employees are able to access email through their personal device such as, mobile phone, laptops, tablet and home computer This 'open access' must be fully understood and individual's must fully understand, comply and accept that with this access comes a degree of personal responsibility.

Any email accessed on a personal phone may contain patient / staff / commercial information all of which is of a sensitive nature and must be treated in a confidential way.

The risks of access using this method are as follows, please note that this list is not exhaustive and is for guidance purposes only:

- Inadequate security settings on a personal mobile / device
- The Trust does not have the ability to ensure that the personal device has up to date operating systems in place. This is up to the individual concerned.
- The ability to auto-forward emails to another account or individual
- Risk of the device being lost / stolen and the data being inappropriately accessed, in such instances the Trust would not be aware of any data loss
- If a device is lost / stolen then passwords must be changed **IMMEDIATELY**
- Information within the phone being 'backed up' to the 'cloud' which presents additional Data Protection implications.
  If a cloud storage solution is used which is outside of the European Economic Area this is a breach of Data Protection Legislation
- Ability to 'screen shot' and forward information on a personal device

4. Responsibilities

The roll out and use of an open access system warrants **individual responsibility** which must be fully understood and accepted.

'Open Access' will allow content to be downloaded from emails, attachments and other Trust content onto a personal device.

Therefore, staff **MUST NOT** under any circumstances:

- **FORWARD** any Trust information to an unauthorised third party or individual.
  This is a breach of Data Protection legislation.

- **DISCLOSE / ALLOW** information in relation to the Trust to be saved / found in the public domain.
  This is a breach of the Data Protection legislation.

- **RETAIN ANY CONTENT** which has been downloaded for work purposes on a personal device. It must be securely deleted once it has been reviewed or the task has been **completed.**

5. Audit and Review

Under 'Open Access' there are no 'controls' in place to prevent downloads or the sending of information via email.

However, there are audit facilities available whereby access can be audited and tracked retrospectively.

6. Reporting of breaches

Whilst there are huge benefits for using electronic devices for the appropriate viewing and sharing of information these do present a risk.

It is important that this risk is balanced and that the Trust has procedures in place to report any breaches of information should this happen.

If an error does occur and information has been incorrectly sent / forwarded to an unauthorised recipient, **then the following actions must immediately take place:**

- Advise line manager and attempt to recall the message via email.
- If this is unsuccessful then sender must contact the recipient.
- Confirm that a document / attachment has been incorrectly sent and request that the information is immediately deleted.
- The recipient will also be asked to confirm via email that has taken place.
- Sender to complete an IRW-1 form detailing incident.

In the event of any queries please contact:
Caroline Smart
Information Governance Lead / Data Protection Officer
Caroline.smart@secamb.nhs.uk

7. Starters & Leavers

It is essential that **ALL** line managers ensure that there is a timely notification and disabling of active directory accounts when staff leave the Trust. This will reduce the risk of emails being erroneously / incorrectly sent.

8. Raising Awareness

It is the line manager's responsibility to ensure that all staff are briefed regularly through team meetings / 1:1's of the correct and appropriate use of Office 365.

The IG Lead will ensure that this guidance is reviewed, published and circulated via Trust bulletins on a 6 monthly basis. This will also include uploading into Content Locker within Trust issued iPads.

APPENDIX A - Policy Awareness

The Trust has a number of existing policies that provide further clarity, a summary / extract of key information from these policies is illustrated below:

Data Protection Policy – as at October 2018

5.9. Contracts of Employment

5.9.1. Staff contracts of employment are produced and monitored by the Trust's Human Resources department. All contracts of employment will include a data protection and general confidentiality clause. Agency and non-contract staff working on behalf of the Trust will be subject to the same rules.

5.10. Disciplinary

5.10.1. A breach of the Data Protection Act 1998 may result in staff facing disciplinary action in accordance with Trust policy.

Information Security & Risk Management Policy – as at October 2018

Encryption

5.17.6. Staff must not use personal IT equipment for business purposes unless there is an identified exceptional need that has been risk assessed and approved by the Trust's IGWG and the SIRO (Senior Information Reporting Officer).

Confidential information must not be processed on such equipment unless the device is encrypted to NHS standards.

Internet & Email Policy – as at October 2018

Information Governance or Other Issues

5.2.1. All such breaches, whether intentional or otherwise will be reported to the Information Governance Lead.

5.2.2. Monitoring will be undertaken to ensure compliance with this policy.

5.2.3. Monitoring will include the interception of personal electronic communications such as email. This monitoring falls within the remit of the Regulation of Investigatory Powers Act 2000 (RIPA).

This generally renders the interception of communications unlawful by non-government organisations without the consent of both the sender and recipient.

However, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 recognise that employers need to be able to monitor systems, without seeking individual consent.

5.3. Internet Monitoring

5.3.1. Monitoring is managed by a software system that automatically records staff internet activity and populates management reports.

5.3.2. The IT Support Manager reviews the management reports and escalates misuse, in line with this policy, to the weekly IT Managers Meeting to identify the action to be taken.

5.3.3. When misuse is suspected, in line with this policy, the Senior IT Manager or chair of the IT Managers Meeting will determine the action to take in reporting the findings to the relevant members of staff or organisations.

5.4. Email Monitoring

5.4.1. Emails are not routinely monitored and will only be investigated under circumstances described in section 2.6 of this policy.

5.4.2. When misuse is suspected, in line with this policy, the Senior IT Manager will determine the action to take in reporting the findings to the relevant members of staff or organisations