North East Ambulance Service NHS
NHS Foundation Trust

Data Encryption Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-2
Version Number	V03
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	19 September 2017
Date Policy Effective From	17 November 2017
Next Review Date	19 September 2020
Keywords	Access control; Business critical information; Encryption; Mobile device; Network; Personal data; Removable media devices; Virtual Private Network (VPN)

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
01	All	Updated in line with DNV recommendations and sections re-ordered with new monitoring table. IT Department responsible for install and management of encryption software across all Trust laptops. Line managers are responsible for the recovery of devices when staff leave.	IG Manager	01 May 2014
02	All	New policy template	IG Manager	August 16
03	All All 4.4	Reference to General Data Protection Regulation. Removal of FOIA. Inclusion of IAO.	IGWG	August 2017
03	4.5 6.2	Floppy drives replaced with removable media. "Mobile" added to first sentence.	Assistant Director IM&T	August 2017
03	4.2	Delegated responsibility to DoF and addition of SIRO.	Director of Finance & Resources	August 2017
03	6.2	Disk drives are blocked.	ISWG	September 2017

This page should not be longer than one single page.

Contents

1. Introduction

Article 32 of the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) states that appropriate technical and organisational measures should be applied to personal data to ensure a level of security appropriate to the risk.

Appropriate software / hardware encryption will be used to protect data to comply with the relevant legislation. This includes the following:

- GDPR 2016
- DPA
- Computer Misuse Act 1990
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

2. Purpose

This document sets out the Trust's policy for the use of encryption for organisational purposes. This policy covers all electronically stored data, held on both static and mobile devices.

This policy is complementary the following Trust Policies and should be used/read in conjunction with them.

- Data Protection Policy - POL-F-IMT-4
- Domain Account Policy – POL-F-IMT-9
- Email Usage Policy - POL-F-IMT-12
- Mobile Computing Policy - POL-F-IMT-15
- Information Security Policy - POL-F-IMT-7
- Information Risk Policy - POL-F-IMT-6

3. Scope

This policy covers all sites and systems operating and utilised by Trust.

The policy applies to any individual employed, in any capacity, by the Trust, volunteer or contractor who holds a Trust domain account.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the confidentiality and security of patient, staff and corporate information Implementation of, and compliance with the policy is delegated to the Director of Finance and Resources who is also the Senior Information Risk Owner.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

The SIRO is also responsible for making sure the trust meets all legislative requirements in relation to information security.

4.4 Assistant Director of IM&T

Has responsibility for:

- The implementation of encryption on all Trust PC's and removable media devices, including the facility for content encryption and the training in its use;
- The purchasing of devices to the required standard, once the user departments have confirmed the funding;
- The support and maintenance of this system via the IT helpdesk function; and
- Managing changes to the configuration of the service.

The Assistant Director of IM&T is also the Information Asset Owner of the encryption software.

4.5 Information Governance Manager

Has responsibility for:

- Developing, maintaining and implementing this policy;
- Approving the business need for writable access to be given to staff for the use of CD/DVD/other writable devices and removable media;
- Monitoring of this policy; and
- Implementing appropriate security solutions to devices and processes.

4.6 Line Managers

Have a responsibility to ensure all current, new and temporary staff are instructed in their responsibilities in relation to the use of removable media devices and work in a manner consistent with this Policy.

4.7 All users

All users are personally responsible for ensuring that they are aware of and compliant with this policy. By signing up to a Domain Account, users will agree to this policy and its guidelines and should be aware that a breach of this policy may be regarded as serious misconduct which would lead to disciplinary action or dismissal in accordance with disciplinary procedures.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Access control	Refers to mechanisms and policies that restrict access to computer resources.
Business critical information	Where the loss of data would have a significant impact on the performance, reputation and operational effectiveness of the organisation. This may include but is not limited to financial, personal, major projects e.g. tender applications.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Mobile device	A portable computing device such as a smartphone, laptop or tablet computer
Network	A group of computers and associated devices that are connected by a communications line or wireless link.
Personal data	Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[1]
Removable media devices	Mobile device that can store data. This will include laptops, palm tops (or personal digital assistants), USB memory sticks, CD/DVD, external hard drive etc.

[1] EU General Data Protection Regulation 2016

Term	Description
Virtual Private Network (VPN)	Allows a user with appropriate authority to connect to the Trusts network from a remote location via the internet.

6. Policy Content

6.1 Areas of risk

The listing below identifies the risks the Trust may be subjected to:

- All Trust PC's are at a potential risk from theft and therefore device encryption will be installed on all PCs across the organisation to ensure the security of personal data and business critical information and to protect against unauthorised access/loss.
- USB connected hard drives have the potential to store large quantities of data and therefore will need to be fully encrypted using device encryption and a justified case made for their use. This will only be considered under specific circumstances and users should seek advice via the IM&T Service Desk.
- Laptops are the most common form of mobile device holding mobile data. This form of mobile computing is increasing within the Trust, and there is a high risk that they can be lost or stolen. A laptop that does not have any form of encryption can allow unauthorised access to the data contained on it, and, so, must be protected. The IT Department will install and manage the encryption software across all Trust laptops.
- Other removable media devices also pose a risk. The loss of any of these devices containing sensitive data would compromise the Trust's information security if there was not robust encryption in place. It is the user's responsibility to make sure that they use these devices with encryption through seeking advice from the IT Department.

6.2 Encryption

All Trust owned mobile computing devices shall be fully encrypted.

Users will only be allowed to write to approved, Trust-owned hardware-encrypted memory sticks. This will be achieved centrally via technical configuration. Staff are responsible for requesting these through the IM&T Service desk and they will be distributed as personal issue items. Staff requesting such devices will remain responsible for the safekeeping and use of the device.

Line managers are responsible for the recovery of devices in the event of staff leaving the organisation as with any other piece of Trust equipment. It will not be possible to read/write data from/to personal devices. Again, this will be achieved at the technical level.

Disk drives are blocked unless a valid business need is identified. This will need a clear recorded business justification to be held on record. Once approval is given, write access will be granted, and the user will be provided with the necessary training to fully encrypt any data written to these devices using “content encryption” All authorisation for writing to these devices must be granted by the user’s manager by the completion of an IM&T Service Desk request

Users’ privately owned mobile computing equipment or related devices (e.g. laptops, PDAs, mobile phones) will not be permitted to connect to the Trust network nor to access Trust network resources. The only exception to this rule will be outlook webmail and via VPN remote access which is tightly controlled technically and monitored through policy and any specific policies allowing privately owned devices.

Other removable devices may be added on an on-going basis if it is deemed that there is a potential need for data to be downloaded to these. However, these will be fully encrypted in line with this policy. All authorisation for reading and writing to any other mobile devices must be granted by the user’s manager by the completion of the relevant IM&T Service Desk form. In cases involving high volumes of data, a risk assessment may be required.

All mobile devices classified within the scope of this policy must be encrypted to the national standard to prevent the possible loss of any Trust data.

Only Trust owned authorised mobile devices may be used, unless exceptions are made under other policies.

7. Training Required for Compliance with this Policy

All staff to receive Mandatory Information Governance Training on an annual basis.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples’ specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England’s Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	Number of encrypted devices against the number of unencrypted devices. Number of data loss incidents.
When will the monitoring be performed?	Every other month.
How are you going to monitor?	Via Ulysses reports.
What will happen if any shortfalls are identified?	Logged in risk registers.
Where will the results of the monitoring be reported?	Information Security Working Group.
How will the resulting action plan be progressed and monitored?	The action plan will be progress by the Information Security Working Group and monitored by the Information Governance Working Group.
How will learning take place	Learning will be via the action plans and monitored by Information Governance Working Group.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Compliance with Trust policy template, format and ratification process	• Style, format and template • Explanation of terms used • Consultation process • Ratification process • Review arrangements • Control, including archiving arrangements • Associated documents • Supporting references • Monitoring section in policy	Assessing all new and reviewed policies against the guidance through presentation to relevant approval groups	Author and approval groups	Finance Committee	Ongoing	To be developed as necessary
Monitoring and reporting on Policy compliance	Number of data loss incidents	Via Safeguard reports	IG Manager	ISWG and IGWG	Bi-monthly	Add to risk registers
Bi - Annual audit of unencrypted devices	No increase	Internal audit programme	IG Manager	ISWG and IGWG	Bi-annual	Add to risk registers

10. Consultation and Review of this Policy

The original Policy was consulted with members of the Compliance and Risk Committee and the Information Governance Working Group in 2011.

This policy has been reviewed in consultation with:

- Information Security Working Group
- Information Governance Working Group

The Policy will be reviewed every three years unless there are significant revisions to be made.

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings

12. References

This document refers to the following guidance, including national and international standards:

- Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents
- EU General Data Protection Regulation 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.legislation.gov.uk/uksi/2000/2699/contents/made

13. Associated Documentation

This policy refers to the following Trust documents:

- Data Protection Policy - POL-F-IMT-4
- Domain Account Policy – POL-F-IMT-5
- Email Usage Policy - POL-F-IMT-12
- Mobile Computing Policy - POL-F-IMT-15
- Information Security Policy - POL-F-IMT-7
- Information Risk Policy - POL-F-IMT-6