Northern, Eastern and Western Devon
Clinical Commissioning Group

Date		15 June 2016		
Policy title		Mobile Devices policy		
Author(s)		Lauren Wellington, Governance Officer John Harle, Governance Manager		
Supporting Executive(s)		Janet Fitzgerald, Director of Governance		
Purpose of Policy		**Decision**	✓	
		Assurance		
		Information		
FOI Status		**Public**	✓	
		Private		
Category of Policy		**Decision**	✓	
		Position Statement		
		Information		
Does this document place Individuals at the Centre		**Y**	**N**	Yes
Actions Requested		Policy approval at Executive Committee		
Which other committees has this item been to?		Staff Forum, December 2015 Information Governance Steering Group, November 2015 Executive Committee 2016		
Reference to other documents		Information Security policy Code of Practice on Confidentiality E-mail and Internet policy		
Have the legal implications been considered?		Yes		
Equality Impact Assessment				
Who does the proposed piece of work affect?		Staff ✓ Patients ✓ Carers ✓ Public ✓		

	Yes	No
1. Will the proposal have any impact on discrimination, equality of opportunity or relations between groups?		✓
2. Is the proposal controversial in any way (including media, academic, voluntary or sector specific interest) about the proposed work?		✓
3. Will there be a positive benefit to the users or workforce as a result	✓	

of the proposed work?		
4. Will the users or workforce be disadvantaged as a result of the proposed work?		✓
5. Is there doubt about answers to any of the above questions (e.g. there is not enough information to draw a conclusion)?		✓
If the answer to any of the above questions is yes (other than question 3) or you are unsure of your answers to any of the above you should provide further information using **Screening Form One** *available from Corporate Services*		
If an equality assessment is not required briefly explain why and provide evidence for the decision.		

NEW Devon CCG has made every effort to ensure this policy does not have the effect of discriminating, directly or indirectly, against employees, patients, contractors or visitors on grounds of race, colour, age, nationality, ethnic (or national) origin, sex, sexual orientation, marital status, religious belief or disability. This policy will apply equally to full and part time employees. All NEW Devon CCG policies can be provided in large print or Braille formats if requested, and language line interpreter services are available to individuals of different nationalities who require them.

Reference to Core Strategies and Corporate Objectives

Core Strategies, we will:	Corporate Objective	Does this report reference to the Core Strategies/ Corporate Objectives	
		✓	X
1. Take joint ownership with partners and the public for creating sustainable health and care services	1.1 Develop people, and those who support them, to value strengths and personal qualities in all that they do	✓	
	1.2 Listen to people and take action on what they say about services	✓	
2. Implement systems that make the best use of valuable health resources, every time	2.1 Innovate to increase productivity and reduce waste	✓	
	2.2 Commission safe services and reduce avoidable harm	✓	
3. Commission to prevent ill health, promote well being and help people with long-term conditions to live well	3.1 Support people to make healthy lifestyle choices and understand the care, treatment and services available to them	✓	
	3.2 Commission services with partners to reduce health inequalities and improve people's lives	✓	

Northern, Eastern and Western Devon Clinical Commissioning Group

Document Status:	Draft
Version:	V2.1 March 2017

DOCUMENT CHANGE HISTORY		
Version:	**Date:**	**Comments (i.e. viewed, or reviewed, amended, approved by person or committee)**
V1	19/06/2013	Initial draft
V1.1	28/05/2015	Amended to reflect organisational and legislation changes
V1.2	03/07/2015	Reviewed by Clare Doble and subsequently amended
V1.3	01/02/2016	Amended to reflect the comments of the IGSG and Staff forum
V1.3	07/06/2016	Amended to reflect comments from clinical members
V2.0	15/06/2016	Approved by Executive Committee
V2.1	29/03/2017	Amended to include Business Continuity requirement of mobile devices
Authors:	Lauren Wellington, Governance Officer John Harle, Governance Manager	
Scrutinised by: (name & title) **Date:**	Clare Doble – Head of Governance 03/07/2015	
Document Reference:	GEN008	
Review date of approved document:	March 2020	

CONTENTS

Linked strategies, policies and other documents

Information Security policy

Code of Practice on Confidentiality

1. Introduction

1.1. This policy applies to all NHS NEW Devon CCG, (hereafter NEW Devon CCG) staff, workers, contractors and all other authorised users of NEW Devon CCG IT resources and email.

1.2. Within the context of the NHS, mobile computing is a term used to describe the use of mobile devices that store or process NHS data. Typically, this will include items such as laptops, smartphones or any mobile telephone that can store data, tablet computers, Personal Digital Assistants (PDA's) and mobile email devices. Mobile computing can bring about many benefits to the NHS. It allows for information to be available whilst working on the move or in remote or home working situations. It can improve the patient care experience and can contribute to the improvement of working lives. These benefits, however, also present a new set of risks. Information is no longer retained within the hospital, General Practice or office; it is moving around the city, the country and potentially even abroad on a variety of devices and through other communication channels.

1.3. Mobile computing devices taken outside secure NHS environments are subject to special security risks: they may be lost or stolen and may be exposed to unauthorised access or tampering. Mobile computing devices taken abroad may also be at risk, for example confiscated by police or customs officials. Mobile devices are also subject to cyber security risks such as rogue software, Malware, key loggers and Ransomware.

1.4. The loss of a mobile computing device will mean not only the loss of availability of the device and its data, but may also lead to the disclosure of patient, employee or other sensitive information. This loss of confidentiality, and potentially data integrity, will often be considered more serious than the loss of the physical asset.

1.5. The NHS holds vast quantities of information and data, data can be defined as raw information that comes into the organisation unorganised and unprocessed, whereas information can be described as data that has been processed, organised or structures in a given contact to make it useful. Where large quantities of NHS data are held on a single laptop (or any other storage medium) risk assessments must consider the impacts of loss of all the data. Note that deleted files should be assumed to persist on the laptop's hard disk.

2. Scope

2.1. The primary mobile computing devices used within NEW Devon CCG are laptop computers and tablets. Consequently this policy is specifically designed for these devices; nevertheless the issues and their solutions

are intended to cover all mobile computing devices, this includes mobile phones/smart phones and PDAs.

3. Purpose

3.1. This policy is designed to identify the risks associated with mobile computing and to describe the controls used to minimise these risks.

4. Policy Statement

4.1. Traditional password protection on a mobile computing device offers limited defence against a determined attacker because the attacker has unconstrained access to the physical device. Modern complex password techniques offer more protection but are not currently in widespread use.

4.2. The physical security controls that are possible within an NHS building environment are not available outside of that environment; therefore if procedural and personal controls of the mobile computing device, in particular a laptop or mobile telephone or tablet, are breached the only effective technical measure that can be applied is data encryption.

4.3. Encryption processes are not difficult but must be used correctly in accordance with defined procedures. In particular the password must be kept separate from the laptop; the password is effectively the encryption key. Data is therefore only protected by encryption when the device is powered off and not in normal use.

4.4. Unauthorised access and tampering to a Mobile computing device, particularly if there are repeated opportunities for access, may:

- lead to continuing (and undetected) compromise of information on the device itself;
- undermine security measures (including the encryption); intended to protect information on the device in the event of loss or theft; and
- lead to the compromising of systems to which the device is connected, for example, an NHS organisation's networked systems that are accessed from the device under an approved remote access arrangement.

4.5. The impact of a breach of mobile computing security may therefore extend far more widely than the device itself.

5. Standard of Acceptable Use for Mobile Devices

5.1 NHS NEW Devon CCG Senior Information Risk Owner (SIRO) is responsible for the Information Security activities undertaken by the CCG and this includes the confidentiality, integrity and availability of NHS information including patient data. The following information governance principles must be demonstrated when using Mobile computing devices:

General Management:

5.2 The CCG's IT Services are provided by DELT Shared Services Limited. DELT is a separate organisation that provides IT Services to the CCG, our GP Practices and Plymouth City Council. DELT are responsible for the management of NEW Devon CCG's laptops and mobile devices which they support.

5.3 Laptops and other mobile devices tend to be more expensive than their fixed location equivalents e.g. laptops are approximately twice as expensive as desktop PCs and require the additional expense of docking stations, encryption etc. Consequently laptops, and other devices, should only be requested where a completed business case justifies their use. If you feel that your job role requires the use of a CCG laptop or device, please discuss your need with your line manager, who will make the decision as to your business needs. If a laptop or device is required, the line manager will need to contact DELT Shared Services.

Registration

5.4 All laptops and mobile devices used for NEW Devon CCG's business or holding NEW Devon CCG information must be uniquely identified and registered this list is held by DELT shared service and made available to the information governance team on request.

Accountability

5.5 Responsibility for the security of NEW Devon CCG's registered laptops and their data must be assigned to individuals (by a designated Asset ID issued by Delt), this can be tracked alongside the employment status of those individuals (e.g. returned when staff leave NEW Devon CCG employment). The exception to this is team laptops who are assigned to an individual within the team. Team laptops should not be used to store any corporate or patient sensitive information.

Management of laptop security functionality

5.6 The installation and configuration of laptop security functionality, including access control, encryption and tamper resistance should be undertaken by appropriately trained DELT staff.

User training and awareness

5.7 Users of mobile devices are required to complete mandatory IG training released by NHS Digital online via **http://www.esrsupport.co.uk/nlms/login.html** which provides basic training on the security of mobile devices and includes safeguarding the device and the individuals' obligation to comply with relevant information and the governance security procedures of the organisation.

Security accreditation

5.8 DELT shared service regularly review the CCG Mobile devices to ensure that they meet these requirements and report monthly the quantity held by the CCG. The CCG **Information Security policy** provides further information.

Authorisation

5.9 Line Managers who authorise the issue of mobile device(s) by default also authorise the use of those device(s) outside NEW Devon CCG premises for the processing of NHS information. Where this is not the case fixed position devices, such as desktop PCs should be issued.

5.10 **Business Continuity planning around mobile devices**

In line with staff terms and conditions of employment under the section entitled normal place of employment, '*exceptionally, and following consultation, you may be required to work elsewhere within the CCG. Such requirements will at all times be reasonable'*. Therefore, it is recommended, although not implicit, that staff issued with mobile devices should take the device home at the end of each working day, whilst maintaining and adhering to information governance principles. It is at the Line Manager's discretion whether their mobile device(s) needs to be taken home, and, especially, conversation would be encouraged over periods of annual leave.

Physical

5.11 At no point should mobile devices be left in an unsecured location or in the care of individuals who do not have appropriate authority to protect the information present on the device, this includes unattended vehicles

Availability

5.12 Continued availability of mobile devices, for operational reasons and because of the costs of replacement, will mean that consistent standards of physical protection will be required for all mobile devices. Please see Appendix A and B for more detailed information regarding security procedures for mobile devices. All relevant staff and contractors should be made aware of this requirement at the start of their employment with NHS NEW Devon CCG.

Virus and Malware protection

5.13 All NEW Devon CCG IT equipment is protected by countermeasures and management procedures to protect against the threat of malicious software. All staff are expected to co-operate with this policy. Users will not install software on the organisation's assets without permission form DELT and their line manager.

5.14 The Virus/malware protection software will automatically update when the laptop is connected to the Network.

Remote Access

5.15 Remote access from a laptop to NHS information systems must be achieved in accordance with the IG Statement of Compliance, NHS IG guidance, and any defined requirements for the protection or use of the NHS information service(s) concerned.

Email

5.16 Person identifiable and sensitive information must not be sent by email if at all possible, however when authority has been given for this type of information to be securely emailed it should be encrypted following process outlined in 5.16 unless otherwise directed by your line manager or information governance team.

5.17 Emails from and to NHSmail Users are automatically encrypted; however emails from an NHS mail user to a non-NHS mail user are not automatically encrypted, and vice versa. NHS.net has enabled a function to send encrypted e-mails to non-encrypted e-mail addresses by the use of [secure] as the first word in the subject (the word secure must be surrounded by the square brackets for the message to be encrypted); this however should only be used in exceptional circumstances. Additional levels of protection include password protection by the sender. Please see the 'Email and Internet policy' for more information about sending sensitive information by email.

Data Storage and use

5.18 Sensitive data, including that relating to patients, should not be stored on a NHS NEW Devon CCG mobile device, including the local drive of a laptop or anywhere on a mobile phone or tablet. Where this is unavoidable for operational reasons this data should be kept to the minimum required for its effective business use in order to minimise the risks and impacts should a breach occur. All NEW Devon CCG data should be placed onto the secure network drive at the earliest opportunity.

Data Backup

5.19 Data held on laptops must be backed up to network storage devices e.g. personal or shared network drives, as appropriate, at the earliest opportunity see Appendix B for further information. It is vital that CCG information is not left on the hard drives of mobile devices as this may lead to loss of CCG data if the laptop is lost or stolen or becomes faulty.

Incident Reporting

5.20 Loss of a NEW Devon CCG mobile device must be reported immediately to the DELT Service Desk and via the CCG's internal incident reporting mailbox **d-ccg.internal-incidents@nhs.net.**

Contact details

5.21 DELT Service Desk – 01752 304425 or ictservicedesk@plymouth.gov.uk alternatively use the Self Service portal.

5.22 Information Governance advice – D-CCG.informationgovernance@nhs.net or alternatively, we can be reached at 01392 356015 or 01392 267777

Secure Disposal and Reuse

5.23 Data stored on NEW Devon CCG mobile devices must be securely erased before the mobile device is reassigned for another purpose or disposed of when redundant. Failure to securely erase data may result in that data being available to the new owner/user of the device. On request DELT will arrange for the secure disposal and destruction, when required, of data and data storage equipment.

5.24 Guidelines for securing mobile devices are included in Appendix A and B.

6. Use of Personal Mobile Devices

6.1 NHSmail may be accessed on a personal device only via the web portal (**www.nhs.net**) at any point; however, it must not be accessed via personal

smart phones, tablets, PDA or personal Laptops e-mail system. This ensures that all e-mails are encrypted in transit and are not saved on the device. Any CCG e-mails saved on a personal device are at risk of confidential data loss if the device is lost, stolen or accessed without authorisation and NHS NEW Devon accept no liability.

6.2 NEW Devon CCG provides staff with appropriate mobile devices in order to fulfil their duties. Due to this, the use of personal mobile devices is not permitted for purposes other than checking CCG email via the web portal. The use of personal mobile devices potentially exposes NEW Devon CCG to unacceptable information security risks such as:

i. Lack of encryption;
ii. Inappropriate access by family or friends members;
iii. Loss or theft and lack of physical security; and
iv. Risk of viruses and malware being introduced to CCG systems through file transfers.

6.3 In exceptional circumstances, should a personal device be required for a limited and agreed period or for clinical staff who work part time for the organisation, permission must be obtained from the relevant Line Manager, the Governance Manager and from DELT prior to use.

6.4 Staff should ensure that any downloaded documents are deleted upon review (such as confidential Board papers and minutes) and ensure that patient identifiable information is not stored on devices under any circumstances. All personal devices used for these purposes should be appropriately secured via a password and appropriate antivirus software and access to the device should be restricted to the individual directly, not family or friends as this would compromise confidentiality.

6.5 Personal devices should not be viewed as an alternative to dedicated CCG devices and should it become apparent that the individual is using their device excessively, an appropriate business case should be submitted and an appropriate device procured.

6.6 Personal use of mobile devices during work hours should be kept to a minimum, particularly with regard to social media. Excessive use may lead to action under the **CCG Disciplinary policy,** which states that misuse of

social networking sites and issues relating to timekeeping may be classed as minor or serious misconduct.

6.7 Care should be taken with mobile devices with cameras and audio recording facilities. Permission should always be sought before taking a photograph or recording audio or video of a member of CCG staff or in an area of work where confidential information may be on display at time of photographing, as the CCG has a duty, under the NHS Code of Confidentiality to protect the confidentiality of staff, as well as patients.

7. Monitoring and Audit

7.1 The Code of Practice for Confidentiality states "*All staff have a responsibility to report breaches, including suspected breaches, of confidentiality."* The **CCG Whistleblowing policy** further states that staff concerns should be raised with line managers or with the Head of Governance or the Chief Nursing Officer and Caldicott Guardian.

7.2 The organisation's Incident Reporting process must be followed where there is a breach or suspected breach of confidentiality. This is set out as part of the **Information Security policy,** which states *"Details [of incidents] will be passed at the earliest possible opportunity to the Information Governance Manager via d-ccg.informationgovernance@nhs.net. All security incidents will be investigated to establish their cause, operational impact, and business outcome."*

7.3 This policy and associated appendices and procedures will be monitored by the Governance Team and both Internal and External Audit during an IG or IT audit may review this and associated policies and procedures. The CCG Audit and Assurance Committee has oversight of all policies in relation to Information Governance.

8. Review

8.1 This policy will be reviewed every three years or at any other time to take into account any changes to legislation that may occur, or guidance from the Department of Health, the NHS Executive or the Information Commissioner.

Appendix A

Security procedures for Smart Phones/Tablets

- The Tablet or Smartphone is provided for work purposes on behalf of NHS NEW Devon CCG. It remains at all times the property of NHS NEW Devon CCG and the device must not be reassigned, transferred or disposed of in any way;
- If the staff member is redeployed or leaves the organisation, the Tablet or Smartphone must be returned to their line manager who will return them to DELT or redistribute to the replacement member of staff;
- For the purposes of security, no one else, including friends or members of your family, may be permitted to use your Tablet or Smartphone. Your account / logon names or passwords must not be divulged to any person;
- In the event that Smartphone or Tablet is lost or stolen, the member of staff must immediately:
    - Report the loss or theft to the Police and DELT shared services on 01752 304425 immediately; and
    - Obtain a Police/Crime reference number and the name of the investigating officer.
- In the event of a member of staff finding their Smartphone or Tablet defective you must report the issue to the DELT Helpdesk on 01752 304425;
- Inappropriate use of Smartphones and Tablets by an employee may be dealt with under NHS NEW Devon CCG Disciplinary procedures;
- It is the responsibility of each staff member to ensure that their device is free from inappropriate/illegal material at all times. Any device containing inappropriate material will be recovered and reimaged and the appropriate line manager informed;
- Data usage will be monitored and where excessive usage is noted, the manager will be advised;
- The staff member must ensure that the minimum data is stored on their Smartphones/tablets in accordance with the Data Protection Act 1998. No information must be stored that breeches Data Protection legislation;
- Removable media must be encrypted if used to store confidential information; and
- Smartphones/Tablets must be stored securely out of sight overnight, both in the office or if used at home.

Appendix B

Security procedures for Laptops

- All Laptops are provided for work purposes on behalf of NHS NEW Devon CCG. They will remain at all times the property of NHS NEW Devon CCG and any device must not be reassigned, transferred or disposed of in any way;
- If the staff member is redeployed or leaves the organisation, the Laptop must be returned to DELT who will reimage the system and redistribute accordingly;
- For the purposes of security, no one else, including friends or members of your family, may be permitted to use your Laptop. Your account / logon names or passwords must not be divulged to any person;
- If a Laptop is left unattended, it must be locked or shutdown;
- Laptops must not be connected to any personal or privately procured hardware peripherals without prior approval from DELT and Information Governance. Printers may be connected as a local device, for example through a USB or LPT port, but it is recommended that advice be sought from DELT or IG before doing so;
- Privately procured software must not be installed on corporate devices;
- All reasonable care to prevent the theft or loss of CCG laptops must be taken. The following security precautions must be considered;

    - Laptops must not be left unattended in public places or left in vehicles;
    - When transporting a laptop, ensure that it is safely kept out of sight. Particular care must be taken on public transport;
    - Do not leave laptops unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access, Make use of room locks and lockable storage facilities where available;
    - Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc and on public transport e.g. buses and trains;
    - Do not use laptops with removable media in places where that media could easily left behind or misplaced;
    - When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots; and
    - Be aware that the use of laptops or tablets in public places will likely draw the attention of those in the vicinity. It is possible that information viewed on a device screen could lead to the unauthorised disclosure of the information to a member of the public.

- In the event that your Laptop is lost or stolen, the member of staff must immediately:

    - Report the loss or theft to the Police and DELT shared services immediately; and
    - Obtain a Police/Crime reference number and the name of the investigating officer.

- In the event of a member of staff finding their Laptop defective must report the issue to the DELT Helpdesk on 01752 304425;
- Full disk encryption must be used with Laptops at all times
- Passwords needs to be as strong as possible whilst still being memorable. NHS Digital (formerly HSCIC) IT Security Good Practice guidelines recommends using a minimum of 8 characters and a mixture of upper and lower case letters, numbers and non-alphabetic characters to create a strong password. Passphrases, being less complex but containing more characters, are also recommended.
- The use of written aide memoirs is not recommended by the NHS Digital guidelines. In particular, passwords hints must never be kept within physical proximity of a mobile device.
- Inappropriate use of Laptops by an employee may be dealt with under NHS NEW Devon CCG Disciplinary procedures;
- It is the responsibility of each staff member to ensure that their device is free from inappropriate/illegal material at all times. Any device containing inappropriate material will be recovered and reimaged and the appropriate line manager informed;
- The staff member should ensure that the minimum data is stored on their Laptops in accordance with the Data Protection Act 1998. No information must be stored that breeches Data Protection legislation;
- Data stored on a laptop is automatically synchronised to the network when the laptop is connected. It is therefore essential to log on to the CCG network regularly to avoid the loss of data if the laptop is lost or becomes faulty, it is also recommended that any data stored on the Laptop Hard Disk be transferred to the appropriate network drive when the laptop is connected to the CCG network;
- Removable media must be encrypted if used to store confidential information; and
- Laptops must be stored securely out of sight overnight, both in the office and in your home.