HEALTHY PEOPLE
living healthy lives
in healthy communities

NHS
Northern, Eastern and Western Devon
Clinical Commissioning Group

Date	December 2014		
Policy title	Information Security policy		
Author(s)	John Harle, Governance Manager		
Supporting Executive(s)	Anne Forbes, Interim Director of Corporate Development and Compliance		
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**	Y
Actions Requested			
Which other committees has this item been to?	Governance Steering Group		
Reference to other documents	Safe Haven policy. Information Security Incident Management process. Checklist guidance for Reporting, Managing and Investigating Information Incidents and Serious incidents Requiring Investigation. Information Risk policy Home Working policy Laptop and Mobile Computing policy Encryption policy E-mail and Internet policy		
Have the legal implications been considered?	Yes		
Equality Impact Assessment			
Who does the	Staff	✓	

proposed piece of work affect?	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	2.1 Innovate to increase	✓	

that make the best use of valuable health resources, every time	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	✓	

HEALTHY PEOPLE
living healthy lives
in healthy communities

NHS
Northern, Eastern and Western Devon
Clinical Commissioning Group

Document Status:	Approved Final
Version:	1.2

DOCUMENT CHANGE HISTORY

Version:	**Date:**	**Comments (i.e. viewed, or reviewed, amended , approved by person or committee)**
0.1	05/03/2013	First draft for approval.
1.0	19/06/2013	Incorporates SIRO comments.
1.1	26/06/2014	Updated to reflect current guidance and processes.
1.2	07/03/17	Updated to reflect change in staff

Authors:	John Harle, Governance Manager
Scrutinised by: (name & title) **Date:**	Clare Doble, Head of Governance and IG Lead
Document Reference:	
Review date of approved document:	March 2018

Linked strategies, policies and other documents	Safe Haven policy. Information Security Incident Management process. Checklist guidance for Reporting, Managing and Investigating Information Incidents and Serious incidents Requiring Investigation. Information Risk policy Home Working policy Laptop and Mobile Computing policy Encryption policy E-mail and Internet policy

1. Introduction

1.1 NEW Devon CCG (hereafter referred to as the organisation) holds and manages a great deal of personal and confidential data, and increasingly information systems are relied on to store and manipulate this information. With this reliance and the many ways by which information can easily be shared across the organisation, with NHS Trusts and other agencies it is important that a consistent approach is adopted to safeguard the information.

1.2 This document describes the organisation's policy on Information Technology (IT) and Information Security, as well as employees responsibilities for the security of information held both on paper and in electronic form, including information systems, removable media (disks, memory sticks, etc), it also references the requirements for transferring information to and from the organisation as described in the organisation's guidance "File Transfer Procedures".

1.3 To provide clarity for the organisation's staff, the Information Security policy has been developed which applies to all staff working on behalf of the organisation irrespective of their location. This policy needs to be read in conjunction with the linked policies and guidance highlighted above.

2. Purpose

2.1 **Objectives**

2.1.1 The objective of the organisation's Information Security policy is to preserve and secure information.

2.2 **Confidentiality:**

2.2.1 Access to data must be confined to those with specific authority to view the data i.e. only an employee with a legitimate business/clinical need to review the information will be permitted to see it.

2.3 **Integrity:**

2.3.1 Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to specification, i.e. the organisation and its IT provider (DELT) will ensure that all systems and architecture are current, secure and fit for purpose.

2.4 **Availability:**

2.4.1 Information must be available and delivered to the right person, at the time when it is needed, i.e. this information will be made available in secure and appropriate manner, rather than an ad-hoc uncontrolled manner.

2.5 **Aim**

2.5.1 The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or used by the organisation by:

- ensuring that all members of staff are aware of, and fully comply with, the relevant legislation as described in this and other policies;
- describing the principals of security and explaining how they will be implemented in the organisation;
- introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities;
- creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business; and
- protecting information assets under the control of the organisation.

2.6 **Scope**

2.6.1 This policy applies to all information, information systems, networks, applications, locations, IT assets, devices and users of the organisation's resources. This includes the organisation's employees working within or external to the CCG, employees of other organisation's, contractors, temporary staff, volunteers or anyone else working on the organisation's business.

3. Responsibilities for IT/Information Security

3.1 Security is everybody's business and therefore everyone has a responsibility to ensure information is appropriate, secure, confidential, accurate and available only to authorised users. This section describes the different areas of responsibilities for ensuring that the organisation's information remains secure. There is a clear division of responsibilities between the Governing Body, Locality and Line Managers, Governance Manager, User Administrators and General Staff.

3.2 The Information Security Policy shall be maintained, reviewed and updated by the Information Governance Manager. This review shall take place on an annual basis or as a result of significant changes in guidance, technology or processes employed.

3.3 **Management of Information Security**

3.3.1 Ultimate responsibility for Information Security rests with the Chief Officer of the CCG. The Senior Information Risk Owner (SIRO) takes overall ownership of the Information Risk Policy. The organisation's nominated SIRO is the Chief Finance Officer.

3.3.2 Information Asset Owners (IAOs) are responsible to the SIRO for controlling the information security assets they are responsible for. On a day to day basis the Information Governance Manager will be responsible for developing and implementing the Information Risk policy and related procedures with the support of IT and the IT provider.

3.4 Directors, Heads of Departments and Line Managers

3.4.1 Line Managers shall be responsible for the security of their physical environments, including the security of information. They are also responsible for ensuring that all current and new, permanent and temporary staff and contractors have appropriate IT equipment and user accounts to carry out their duties.

3.4.2 Line Managers should ensure that staff are aware of:

- their personal responsibilities for information security;
- how to access advice on information security matters; and
- Information Security policies that are applicable in their work areas.

3.4.3 In particular line managers should ensure that:

- staff using computer systems/media are trained in their use;
- no unauthorised staff are allowed to access any of the organisation's computer systems or information stores as such access could compromise information integrity;
- the IT provider is notified of new employees and leavers to allow access rights to be appropriately established from effective dates for shared data folders and to terminate access when no longer required;
- procedures are in place to minimise the organisation's exposure to fraud, theft or disruption of its information systems - such as segregation of duties, dual control or staff rotation in critical susceptible areas;
- current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability;
- all staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment;
- information security breaches are reported to local IT helpdesks and the information governance team (on 01392 356055 or d-ccg.informationgovernance@nhs.net .This is in addition to reporting them, using the corporate Incident reporting process, reporting them via d-ccg.incidents@nhs.net ; and
- guidelines on legitimate relationships are adhered to when

determining which individuals are to be given authority to access specific information. Levels of access to specific systems should be on a job function need, independent of status.

3.5 Staff

3.5.1 Employees, including those under contract and agency staff, are responsible for conforming to the IT/Information Security policy and as such are required to bring to their manager's attention areas of concern regarding information security. Each user shall be responsible for the operational security of the information systems they use.

3.5.2 Each system user must comply with the security requirements that are currently in force, and must also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

3.5.3 Contracts with external contractors that allow access to the organisation's information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

3.5.4 All staff must comply with security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action. As such, all staff have a responsibility for ensuring that they are aware of, and fully understand, all information security requirements defined in this policy and its associated policies and documents. Any questions or concerns should be brought to the attention of their line manager or the Information Governance Manager.

3.6 Information Governance Manager

3.6.1 The Information Governance Manager for the organisation is responsible for the implementation and enforcement of the IT/Information Security policy in partnership with our Head of IT and has organisational security management responsibilities for:

- ensuring that the information security is effectively implemented throughout the organisation;
- ensuring that appropriate information security controls are applied to new computer systems on the basis of risk and cost benefit;
- developing and enforcing detailed procedures to maintain information security and governance;
- ensuring compliance with relevant legislation;
- reporting material information security incidents to the Head of Governance, SIRO and Caldicott Guardian; and
- providing an advisory service on information security and information

governance.

3.7 IT Managers and IT Project Managers

3.7.1 All IT Managers and IT Project Managers should understand the risk to computer assets and the information that is held on them, deploying appropriate security measures to reduce the threat and to reduce the impact of a threat that materialises in a given project or area of work.

3.8 Information Asset Owners (IAO)

3.8.1 Amongst other things, IAOs are required to ensure compliance with the organisation's IT/Information Security policy and to:

- provide a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection notification;
- put in place defined security and system management, including documented processes for access control, records management and reports;
- implement appropriate levels of access for staff/users using role based access controls (RBAC);
- ensure staff receive appropriate training;
- liaise with the Head of ICT and IT Service Providers over 3rd party access;
- collaborate with internal audit over system security reviews; and
- manage upgrades to systems in partnership with DELT.

4. Legislation

4.1 The organisation is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the organisation, who may be held personally accountable for any breaches of security for which they are responsible.

4.2 The organisation will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998);
- The Copyright, Designs and Patents Act (1988);
- The Computer Misuse Act (1990);
- The Health and Safety at Work Act (1974);
- Human Rights Act (1998);
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000;

- Health & Social Care Act 2012; and
- Lawful Business Practice Regulations 2000.

5. Policy Framework

5.1 Information Security Awareness Training

5.1.1 Information security awareness training will be included in staff induction and mandatory training.

5.2 Contracts of Employment

5.2.1 Security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause to be signed by all staff.

5.3 Security Control of Assets

5.3.1 Every information asset, (hardware, software, application or data) will have a named custodian (Information Asset Owner) who will be responsible for the security of that asset.

5.3.2 Each PC or device (such as smartphone) will be allocated to a named individual. The responsibility for PCs shared by several staff will lie with locality or line managers.

5.4 Access Controls

5.4.1 Only authorised personnel who have a business need will be given access to restricted areas containing information systems, i.e. information is not available by default to all staff but solely to those employees whose role requires it. Access to patient information in particular will require a legitimate relationship to exist in order to justify this access. Further details regarding legitimate relationships can be found at:

5.4.2 http://www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/impguidpm/ig/legitrelate

5.4.3 Applications for new or revised access controls must be supported by the user's line manager and approved by the Information Asset Owner.

5.5 User Access

5.5.1 Access to information will be restricted to authorised users who have a business need to access that information i.e. Role Based Access

Controls will be deployed (RBAC).

5.6 User Accounts

5.6.1 Individual, named accounts for all network and system users ensure that proper auditing of accesses made can be maintained. Usernames and passwords should not be shared for any reason.

5.6.2 The organisation does, however recognise that in some cases generic or shared accounts are required but this will not be a standard approach and the need will be assessed on a case-by-case basis according to business need.

5.7 Passwords

5.7.1 In no circumstances must passwords be attached to devices, whether laptops, smartphones, Registration Authority smartcards or “key fob” authentication tokens. Passwords must not be attached to the cases or bags used to transport the devices. Additionally, authentication devices (key fob or smartcard) should not be stored with a laptop.

5.7.2 As with laptops, the organisation is making steps to ensure that all data on smartphones is secured by means of encryption.

5.7.3 Passwords have a role in protecting systems from unauthorised access and are most effective when they:

- carry no meaning;
- are not names, nor easily guessable;
- are changed regularly and are not related to previous passwords;
- are a minimum of 8 characters;
- are a mixture of letters, numbers and symbols;
- are kept secret;
- are not PASSWORD / VISITOR / GUEST or similar;
- are not shared; and
- should be memorable, preferably through a cryptic association with the user

5.8 Computer Facilities Access Control

5.8.1 Access to computer facilities will be restricted to authorised users who have a business need to use the facilities.

5.9 Application Access Control

5.9.1 Access to data, system utilities and program source libraries will be controlled and restricted to authorised users who have a business need to use the applications, i.e. RBAC applies. Additionally, authorisation to use an application will depend on the availability of a license from the supplier.

5.10 Equipment Security

5.10.1 In order to minimise loss of, or damage to, IT assets, equipment should be physically protected from security threats and environmental hazards, i.e. laptops and phones should not be left in insecure areas such as on view in cars or on desk tops when not in use.

5.10.2 Line managers are responsible for ensuring the provision of IT equipment to allow staff to carry out their duties and for the return of IT equipment to the organisation's IT team when this equipment is no longer required.

5.10.3 Additional details on equipment security can be found in the organisation's Laptop and Mobile Computing Security policy.

5.11 Computer and Network Procedures

5.11.1 Management of computers and networks will be controlled by standard procedures that have been authorised by the Head of Delivery.

5.12 Security Incidents, weaknesses and status reporting

5.12.1 All IT/Information Security incidents and weaknesses, suspected or material, are to be reported to the organisations Information Governance Team (01392 356055 or d-ccg.informationgovernance@nhs.net). All security incidents will be investigated to establish their cause, operational impact, and business outcome. Material breaches and serious potential breaches which highlight gaps in policy, training or awareness will be reported to the SIRO. Minor incidents will be dealt with by the Governance Manager and IT team. Significant and serious incidents will be dealt with in line with the organisation's Incident Management processes.

5.12.2 See Appendix A for Guidance and Appendix B for report form.

5.13 Protection from Malicious Software

5.13.1 The organisation will ensure that software countermeasures and management procedures are implemented to protect itself against the treat of malicious software (computer viruses etc).

5.13.2 All staff will be expected to co-operate fully with this policy. Users must not install software on the organisation's property without permission from the Head of IT. Users breaching this requirement may be subject to disciplinary action.

5.14 Removable Media such as Memory Sticks

5.14.1 Removable media containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

5.14.2 If the organisation's data is to be stored or transmitted on such devices, encryption should be used – see the NEW Devon CCG Encryption policy.

5.14.3 Please note that it is forbidden to store patient, staff or other sensitive data on an unencrypted device.

5.15 **Purchase of new equipment, software and systems:**

5.15.1 All projects involving the purchase of new equipment/software must consider the security aspects. The operational requirements and strategic implications of new systems should be established, documented and tested prior to their acceptance. Managers are responsible for informing the IT Department of new projects that have an IT component so that sufficient time is available for this review. The time required will vary dependent upon the scale and complexity of the project.

5.15.2 Managers responsible for the organisation's projects with a dependency upon IT must complete a project template document (available via the IT Department). This will be used to register the project with the IT Steering Group and to ensure that appropriate support is available.

5.16 **Mobile Hand Held Devices (Smartphones/iPads)**

5.16.1 Mobile devices should be password protected and include a time out facility whereby the device locks after a set-time period requiring the password to be re-entered.

5.16.2 Mobile devices must be capable of remotely being wiped should they be lost. Mobile devices must also be encrypted. If you do lose your mobile device you must inform the IT Helpdesk as soon as possible so that it can be remotely de-activated.

5.16.3 Mobile devices should not be left unattended.

5.16.4 All mobile devices must be authorised for use – by your Line Manager. (DO NOT use your personal mobile phone [non-NHS owned] to record sensitive work related information).

5.16.5 All staff using iPads must read and comply with the organisation's iPad User Guidance, issued with the devices.

5.17 **Use of (personally owned) Computers, Laptops, Smartphones and**

Tablet Devices

5.17.1 Personally owned devices of any kind must not be used to store confidential or sensitive information.

5.17.2 If you need to use a computer at home discuss obtaining an encrypted organisation laptop with your line manager.

5.17.3 Remote log-on security tokens must not be shared.

5.17.4 All remote users must be approved by their Line Manager.

5.17.5 Particular care must be taken when accessing web-based email services such as NHS Mail. DO NOT transfer sensitive or confidential emails and attachments onto non-NHS owned computers.

5.18 Instant Messaging and Social Networking Services

5.18.1 Instant messaging services allow users to share files and transmit information via the Internet. These services are often not encrypted and must not be used without the authorisation of the IT department.

5.18.2 Internal instant messaging (LYNC) services are in the process of implementation throughout the organisation. The LYNC system is not intended as a direct replacement for e-mail, instead it is an enhancement which helps to improve immediate communications using short messages.

5.18.3 The LYNC system must not be used for conversations which involve business decisions which may need to be evidenced at a later stage.

5.18.4 Sensitive data such as usernames, passwords, account numbers and other personal data must not be passed via instant messaging.

5.18.5 The LYNC system has the facility to share desktops and files, but it is highly recommended that other methods such as NHS mail are used, as the integrity of your desktop information is at risk.

5.18.6 LYNC can be used for limited personal purposes however, such use should be confined to meal breaks and personal time.

5.18.7 Corporately provided instant messaging must only be used to internally or to approved partners

5.18.8 The organisation does not read the messages and e-mails of all users however, may apply manual and/or automatic message monitoring, filtering and rejection systems as appropriate and deny transmission of messages with content that is considered by the organisation to be unacceptable. All messaged which have suspected inappropriate content will be examined.

5.18.9 Social networking services such as “Facebook” must not be used unless there is a specific NHS business requirement. The use of social networking sites should be approved by the IT department. These types of services must not be used to share confidential or sensitive information.

5.19 Use of Cloud Computing services

5.19.1 “Cloud computing” services where documents are stored on Internet based services such as “Google Docs”, “Dropbox”, “and SkyDrive” must not be used to store NHS documents. The security, location or organisational indemnity from legal action in relation to data hosted on these services cannot be guaranteed.

5.19.2 Cloud computing services are undergoing a period of rapid development and increasing popularity. It is likely that local NHS partners may utilise Cloud based services to share and host documents but these must not be used to exchange sensitive information without prior authorisation and approval must be in place with regard to the use of such a service as an approved data flow.

5.19.3 Further information on procuring and using cloud computing services can be found on the Information Commissioner’s website at www.ico.org.uk.

5.20 Data Storage

5.20.1 It is important that computer files are saved in the correct place; generally this is to a network file storage area (network drive). Using a network drives ensures that files are secure, that they are backed up and can be recovered should one be corrupted or accidently deleted.

5.20.2 Confidential and sensitive information should always be saved to a network drive if at all possible, if it must be saved to the local hard drive of a computer or laptop (or any other device) then that device **must** be encrypted. Users breaching this requirement may be subject to disciplinary action that could lead to dismissal.

5.20.3 All staff should have file storage area on their DELT network; this is a personal storage area in which information that does not need to be shared with other members of staff should be saved.

5.20.4 In circumstances where more than one person needs access to the same file a shared network drive should be created. Contact the DELT Helpdesk to request a shared network drive. Care must be taken with this type of network drive as all those with access to them can see all the files within it, therefore line managers will need a strategy to ensure only authorised staff have access to sensitive or confidential information.

5.21 Transmission of Data

5.21.1 The security of the transmission of data, particularly that containing patient identifiable elements, clinical content or personal details of any kind is paramount.

5.21.2 Whether physical (e.g. hardcopy patient notes) or electronic data (email, fax, data exports, or disk/tape, etc), all transmissions within the CCG or to any external bodies must be secure.

5.21.3 The key principles are shown in the bullet points below:

- NHS mail may be used for attachments up to 20mb;
- ~~the~~ NHS Digital provides a secure file transfer service, this is appropriate for larger files transfers;
- faxes must be to secure faxes with nominated persons standing by to receive the transmission;
- data on media such as tape, disk, memory stick etc, must be encrypted and sent by either secure courier services or by hand by the organisation's staff; and
- SecureSend can be used to send secure e-mails to e-mail addresses not part of the secure e-mail system (nhs.net, pnn.police, gsi.gov).

5.21.4 Staff sending or transmitting information, must ensure that the recipients of such data understand and comply with the relevant legal and best practice standards.

5.21.5 The organisation's employees expecting to receive such data from colleagues, both internal and external, should take steps to ensure they are familiar with arrangements for securely receiving data.

5.22 Monitoring system access and use

5.22.1 It will be possible to access audit trails of system access and use. In the event of a suspected breach in policy, procedure or confidentiality these audit trails may be used as forensic evidence. Audit trails may also be reviewed routinely for security and effective management purposes.

5.23 Accreditation of Information Systems

5.23.1 The organisation will ensure that all new information systems, applications and networks are compliant with the organisation and DELT security policies before implementation.

5.23.2 Suppliers of any systems must satisfy the organisation that relevant clauses on Freedom of Information, Data Protection Act, Information Security and Incident Management are present in any contracts. All government framework suppliers are required to satisfy these requirements before being accredited and added to framework catalogues.

5.23.3 Any employee engaging a non-framework supplier must gain assurance from the supplier that these criteria are met.

5.24 System Change Control

5.24.1 Significant changes to information systems, applications or networks must be reviewed and approved by the Head of ICT in conjunction with other relevant service leads prior to implementation.

5.25 Intellectual Property Rights

5.25.1 The organisation will ensure that all information products are properly licensed and approved by the Head of IT and/or IT Provider. Users must not install software on the organisation's property without permission from the Head of IT and the relevant owner or licensee. Users breaching this requirement may be subject to disciplinary action.

5.26 IT equipment and Media Disposal

5.26.1 Computer assets must be disposed of securely and promptly as soon as they are deemed redundant and unsuitable for redeployment i.e. to Waste Electrical and Electronic Equipment (WEEE) standards. In addition to PCs, servers and laptops, this includes removable computer media such as tapes and disks, memory sticks and printed reports.

5.26.2 The organisation and its IT Providers have arrangements with certified disposal companies to ensure that no assets capable of compromising the security of the organisation can fall into the wrong hands.

5.26.3 If you have any IT equipment that needs to be disposed of, please contact the organisation's IT Team.

5.27 Business Continuity and Disaster Recovery Plans

5.27.1 The organisation will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

5.27.2 All critical systems will have a written back-up procedure and disaster recovery plan. This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. This is the responsibility of the Information Asset Owner.

5.28 Clear Desk policy

5.28.1 Any confidential information must be placed out of sight, in locked cabinets/drawers when not in use.

5.28.2 Likewise all offices/rooms which contain personal data should be locked when not in use. Passwords or usernames must not be left on desktops or attached to PCs or laptops.

5.29 Policy Audit

5.29.1 This policy will be subject to audit by both internal and external audit as and when required.

5.30 Review Process

5.30.1 The policy will be reviewed periodically. In addition, the policy will be reviewed in the light of any new statutory, regulatory or best practice guidance.

5.31 General Physical Security

5.31.1 In public areas or rooms where the public have regular access (such as Reception Areas), terminals or screens should be placed facing away from the normal access routes.

5.31.2 Staff should use a password protected screensaver, or lock their workstation if there is someone present who is not authorised to view information displayed or if they leave their workstation for any period of time (the network enforces a password protected screensaver after 5 minutes – attempts should not be made to deactivate this).

5.31.3 Computer files holding confidential, sensitive or important business data must be stored on network drives (such as N:\ or X:\) NOT THE LOCAL PC DRIVE (such as C:\) so that they are held in a secure environment and regularly backed up; computer files holding confidential or sensitive information must be protected from unauthorised access by storing the file in the appropriate location on the network. All departments have shared secure folders / storage areas on the network that are restricted from general access. Discuss the location of these secure folders with your line manager.

5.31.4 Personally owned equipment must not be connected to the organisation’s network (including smart phones and tablet devices) unless prior authorisation is granted via email from the IT Lead or nominated deputy. Sensitive data could be transferred to the phone which may be un-encrypted.

5.31.5 No computer equipment is to be repaired or dismantled in any way, other than by members of the IT team or an authorised maintenance company (through the IT department).

5.31.6 Staff must ensure that visitors are controlled / supervised whilst using or accessing CCG IT facilities.

5.32 Further information

5.32.1 Further information and advice on this policy can be obtained from the Information Governance Team, who may be contacted on 01392 356055 or d-ccg.informationgovernance@nhs.net

6. Implementation

6.1 Once approved, the policy will be made available to all staff via the organisations intranet. The existence of the policy and its relevance to staff will be communicated via the organisation's standard methods.

6.2 Training

6.2.1 Training will be delivered in accordance with the organisation's requirements by the most appropriate and cost effective methodology.

6.3 Monitoring and Audit

6.3.1 All staff have a responsibility to report actual or suspected information security breaches to their, line manager and the Governance team or directly to the Information Governance Manager.

6.3.2 Breaches of security and/or confidentiality are a serious concern and a failure to adhere to this policy may result in disciplinary action.

6.3.3 It is a criminal offence to knowingly or recklessly misuse any information or allow others to do so.

Appendix A – Information Security Incident Management

Process

1.1 This process will be maintained in line with the main organisational incident process.

1.2 All organisation staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

1.3 All staff must be aware of their responsibilities in terms of making the organisation aware of any material or suspected breaches and the mechanisms in place to do so. All breaches or suspected breaches of information security, confidentiality or of this policy must be reported through the organisations incident reporting process.

1.4 This policy also documents the organisation's expectations of its IT provider and other IM& providers.

2. Implementation

2.1 An information security breach is defined as any incident which compromises any of the 3 fundamentals of security – confidentiality, integrity and availability. Example breaches might include a computer virus or Trojan being found on a PC or network drive; the loss of patient identifiable data or the loss of a mobile device such as a laptop or a smartphone.

2.2 The definition of an information security breach is different to that of Serious Incident Requiring Investigation (SIRI) which is generally defined as:

- an adverse incident when a patient, member of staff, or members of the public suffers serious harm, or unexpected death (or the risk of death or injury) on hospital, other health service premises, premises where health care is provided including in a patient's own home. In the case of those in receipt of mental health care services this may occur anywhere in the community;
- where actions of health service staff are likely to cause significant public concern; and
- any event that might seriously impact upon the delivery of service plans and/or may attract media attention and/or result in a settlement following litigation and/or may reflect a serious breach of standards or quality of service.

2.3 Not all information security breaches will turn out to be SIRIs, however in the first instance each security breach will be considered as a SIRI by the Information Governance (IG) Team – this may be downgraded once the exact nature of a breach is determined.

2.4 It is important that suspected or actual information security breaches are immediately notified to the IG Team on 01392 205205 as SIRIs must be reported to NHS Digital within 24 hours.

3. Reporting Incidents

3.1 Staff will make their line manager aware of any security breach, both material and suspected, at the earliest opportunity.

3.2 The line manager should carry out an immediate risk assessment of the incident and where appropriate take immediate steps to ensure the personal safety of staff, patients and members of the public.

3.3 The line manager should take immediate action (where practicable) to terminate the incident i.e. stop the situation getting worse.

3.4 The incident should then be logged with the local IT Helpdesk as a high priority. Informing the helpdesk call handler that the call is regarding a security incident should ensure a high priority is allocated to it but, if the Helpdesk is unwilling to treat the call sufficiently seriously, incidents may be reported directly to the Information Governance Manager on 01392 356022 or d-ccg.informationgovernance@nhs.net.

3.5 The call detailing the incident will be flagged for attention of the IT Provider / IT Support Manager or Operations Manager.

3.6 Breaches related entirely to failures of the IT Provider's systems/networks etc. will be dealt with immediately by the provider systems/networks/support teams for immediate resolution.

3.7 Details will be passed at the earliest possible opportunity to the Information Governance Manager. All security incidents will be investigated to establish their cause, operational impact, and business outcome.

3.8 Potential or very minor breaches linked to the actions of an individual will be dealt with as appropriate, perhaps by making that individual aware of what has occurred and reminding them aware of their obligations in terms of security.

3.9 More severe breaches will be flagged to line managers and other management as appropriate.

3.10 Details of a material breach will then be passed to the Information Governance Manager along with details of any actions taken by the IT Provider and also recommendations on any further corrective actions to be taken by the CCG.

3.11 Breaches related to external service providers will be passed to the relevant helpdesk or manager at the earliest opportunity.

3.12 All incidents will be logged and a report made to the Senior Information Risk Owner (SIRO) and Caldicott Guardian (if the incident relates to Patient information).

4. Obligations to IT Providers

4.1 The CCG expects DELT to ensure that they have an appropriate information security policy, procedures and arrangements for securing the organisation's assets and information as it would do its own such assets and information.

4.2 IT Provider Support and Operations Managers should, while taking action to mitigate any breach, make the breach known to the organisation's Information Governance Manager at the earliest opportunity.

4.3 Evidence or other supporting information should be made available as soon as practicable.

HEALTHY PEOPLE
living healthy lives
in healthy communities

NHS
Northern, Eastern and Western Devon
Clinical Commissioning Group

Appendix B: Information Governance Incident Summary Report

Owner: **Date:**

Classification	**NHS Confidential**
Report for	
On behalf of	
Incident no (office use only)	
Type of breach (office use only)	
Prepared by	
Report date	

Incident summary – key points

Date and time of the incident	
Date breach identified	
Breach Type	
Data Controller	
Other Data Controller affected	
Description	
Number of records involved	
Type of records and impacted and sensitivity	

Number of individual data subjects affected	
Initial assessment of incident level	
Who has been notified	
Level of investigation/confirmation DoH guidelines used	
Information and evidence gathered	
Method of investigation used	RCA
Duty of Candor – have data subjects been notified, if not why not?	
Potential for media interest	
FINDINGS	
Evidence of good practice	
Are there consequent risks if so how will they be managed	
Contributory Factors	
Root Causes	
Lessons Learned	
CONCLUSIONS	
Recommendations	
Further actions required/follow up	