<table>
<thead>
<tr>
<th><strong>Executive Summary</strong></th>
<th>• This Policy defines the Security requirements for data encryption upon laptops, physical media and Secure File Transfer within the CCG</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date of ratification</strong></td>
<td>Executive Team Committee  22nd October 2013</td>
</tr>
<tr>
<td><strong>Document Author(s)</strong></td>
<td>Collette McQueen</td>
</tr>
</tbody>
</table>
| **Who has been consulted?** | Henry Black 1st October 2013  
Senior Management Team 2nd October 2013  
Staff Consultation 9th October 2013  
Executive Team Committee 22nd October 2013 |
| **Was an Equality Analysis required?** | No |
| **With what standards does this document demonstrate compliance?** | Data Protection Act 1998 |
| **References and associated CCG documentation** | THCCGIG8 Information Governance Policy, THCCGIG9 Information Governance Strategy THCCGIG20 ICT Policy, THCCGIG38 Information Lifecycle management policy, THCCGIG43 Personable Identifiable Date |
| **List of approvals obtained** | Senior Management Team 2nd October 2013  
Executive Team Committee 22nd October 2013 |
<p>| <strong>Recommended review period</strong> | 22nd October 2015 |</p>
<table>
<thead>
<tr>
<th>Key words contained in document</th>
<th>Governance, encryption, data,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is this document fit for the public domain? Y / N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Contents

1 Introduction......................................................................................................................................... 4
2 Policies statement .............................................................................................................................. 4
3 Scope .............................................................................................................................................. 5
4 Who this policy applies to ............................................................................................................... 5
5 Definitions used in this policy ........................................................................................................ 6
6 Recommendations for Independent Contractors ........................................................................ 7
7 Initiation, development and review of the policy ......................................................................... 7
8 High-level Security Principles ...................................................................................................... 7
9 Specific Policy Requirements ....................................................................................................... 8
10 Accounting & Audit ..................................................................................................................... 10
11 Configuration of Trust Equipment ............................................................................................. 11
12 Encryption of Portable Computing Devices ............................................................................. 11
13 Encryption of Portable Storage Devices ................................................................................... 11
14 NHS Approved Encryption Product ............................................................................................ 12
15 Secure File Transfer (SFT) .......................................................................................................... 12
16 Transferring Data and Information using Removable Media .................................................. 12
17 Guarding Against Loss or Theft of Equipment ........................................................................ 14
18 Reporting Loss or Theft of Equipment ......................................................................................... 15
19 Dissemination ............................................................................................................................... 15
20 Implementation of this Policy ...................................................................................................... 15
21 Advice and Guidance ................................................................................................................... 15
1 Introduction.

The Data Encryption Policy (the Policy) defines the security operational requirements of the CCG to secure all data held upon portable computing devices, portable storage devices and removable media. It also applies to all data being transported beyond the physical security of the CCG.

Data encryption upon laptops, other portable devices and transportable media, is required as traditional password protection on such devices offers limited defence against a determined attacker, simply because the attacker has unconstrained access to the physical device. In addition, the physical security controls that are possible within an NHS building environment are clearly not available outside of that environment. Thus, data encryption provides the only measure that can be relied upon to preserve the CCG data protection requirements if a laptop, portable storage device or transportable media is lost or stolen.

The Department of Health and NHS Connecting for Health provide well defined guidance on data encryption based, in part, upon recommendations made by CESG. This Policy reflects such guidance.

As it is a requirement for the CCG to comply with the Information Security Standard ISO 27002, this Policy complies with all the relevant requirements specified by this Standard for mobile computing and data encryption. More specifically, this Policy complies with ISO 27002, Sections 10, 11 and 12.

Finally, this Policy is concerned with protecting data in transit, whatever the media employed to store such data. For example, it applies to specific devices such as portable computers and removable media that, although they may be only used on site, are easily lost or stolen.

All staff and third-parties will be expected to comply with this Policy in full.

2 Policies statement

The Policy is intended to achieve the following Information Security Objectives:

Confidentiality – Access to the CCG data and information must be confined to only those users with a specific authority to view the data (i.e. only an employee with a legitimate business/clinical need to view or access information will be permitted to do so). Encryption of such data will ensure that only valid users are able to decrypt and view the data;

Integrity – the CCG data and information is to be complete and accurate. Encryption of data will maintain integrity by preventing the unauthorised modification of such data;

Availability – the CCG data and information must be available and delivered to the right person, at the right time when it is needed (i.e. this information will be made available in a secure and appropriate manner). Encryption of data allows its transport from one location to another, and from one person to another in a secure and timely manner; and

Accountability – Users are held responsible for their access to and use of the CCG data and information. Accountability is implemented by ensuring that only valid users are able to gain access to encrypted data via use of appropriate user authorisation credentials. In addition, accounting and audit mechanisms, where available, will be employed to log access to all relevant devices and data.
3 Scope

This Policy is applicable to all the CCG (including local presences) and hosted organisations IT and IS computer systems, databases, facilities and networks. It is also applicable to third-party IT and IS computer systems, databases, facilities and networks that are employed to provide services to the CCG.

This Policy applies to all the CCG information, information systems, networks, application systems and users. This Policy applies to all sites used by the organisation and applies to all those having access to information, either on site or remotely. This includes, but is not limited to: staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

This Policy is applicable to all electronic data held on laptops, portable devices and/or media in transit – whatever it’s confidentiality and sensitivity requirements. For the avoidance of doubt, the type of data to which this Policy applies is:

Person Identifiable Data (PID) – any data that can be used to identify a patient in any way. This includes pseudonymised data that, although itself may not identify an individual, can be used in conjunction with other data and/or systems to identify a patient;

Commercial and Sensitive Data - any data that may be produced or held by the CCG and that may be regarded by the CCG or the originating source or recipient as commercially sensitive or sensitive for some other reason (e.g. Tender documents or financial and contract information, etc.); and

All Other Data – this includes any other data and information that concerns the CCG in any way and includes word-processing files, spreadsheet files and email data to name but three examples.

Staff and third-parties will only be allowed to transport PID data in accordance with the requirements outlined later in this Policy.

Staff and third-parties will not be permitted to store any PID data on laptops or any other portable storage device.

Staff and Third-parties who believe that they have a requirement to store and process PID data on laptops and other storage devices will be required to apply for appropriate policy waivers using the Policy Waiver Procedure.

All Staff and third-parties must be aware that remote access to PID data will be required via the RiO application, and all Users of PID data should contact their Service Manager to assess how their business requirements can be met by this Strategic solution.

4 Who this policy applies to.

4.1 Staff (including temporary staff)

All staff employed by the CCG have a responsibility to ensure that:

They work to the most up to date and relevant corporate and local Information Security policies; and

They work to the most up to date and relevant Information Governance policies.
4.2 Responsibilities of Employees

All employed staff are responsible for carrying out their duties in line with the policies, to note new or amended policies and to contribute to policy making as necessary.

4.3 Managers

All staff with a supervisory role have a responsibility to ensure that:

All staff have been shown how to access this policy on the Intranet policy library;

Local induction of newly employed staff includes being made aware of the relevant policies and how it impacts their own roles; and

Policies that they are responsible for are reviewed appropriately on an ongoing basis and are disseminated and implemented within services as directed.

5 Definitions used in this policy

5.1 Asset

Any information system, computer or programme owned by the organisation.

5.2 Authorisation

The granting or denying of access rights to network resources, programmes or processes.

5.3 Caldicott

A set of standards developed in the NHS for the collection, use and confidentiality of patient-related information.

5.4 Internet

A global system connecting computers and computers networks. The computers are owned separately by a range of organisations, government agencies, companies and educational institutes.

5.5 Information Governance Toolkit

A series of requirements, produced jointly by the Department of Health and NHS Connecting for Health.

5.6 ISMS – Information Management System

An information security management system (ISMS) standard to help establish and maintain an effective information management system, using a continual improvement approach.

5.7 Network

A system of interconnected computers which allows the exchange of information network connection. An individual's access to the network usually involves password checks and similar security measures.
5.8 Software

Computer programmes sometimes also called applications.

5.9 Virus

An unauthorised piece of computer code attached to a computer programme which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.

5.10 Person Identifiable Data (PID)

PID is data that contains sufficient information to relate the data to a specific patient.

5.11 Portable Computing Device

Any mobile device capable of carrying and/or processing data. This includes laptop computers, PDAs, an increasing number of mobile phones.

5.12 Portable Storage Device

A device capable of storing data that can be moved between host computers. This includes: Portable or External hard disk drives, USB “pen-drives”, ZIP drives, digital cameras, MP3 players, etc.

5.13 Removable Media

This include tapes, floppy discs, removable or external hard disc drives, optical discs (DVD and CD), solid-state memory devices including memory cards and pen drives, etc. There might be some overlap in the definition of certain device.

6 Recommendations for Independent Contractors

As all staff and third-parties are expected to comply with this and other policies, there are no additional recommendations.

7 Initiation, development and review of the policy

This Policy meets all relevant requirements in its initiation, development and review.

8 High-level Security Principles

All staff and other users including third-parties handling the CCG Data must be aware of the following risks and issues:

Reputational Risk – loss of any Data could have an adverse impact upon the reputation of the CCG. The confidence that the CCG currently enjoys from the NHS Executive, patients and other key stakeholders could be seriously undermined;

Patient Distress – loss of PID data could lead to severe stress and trauma for our patients as information on any medical conditions could be made public. Patients could take legal action against the CCG further undermining public confidence. Some four principal patient risks have been identified by the Data Sharing Review, 11 July 2008, conducted at the request of the Prime Minister:
Indignity – unnecessary exposure of facts/suspicions, for example, disclosure of a medical condition that may cause embarrassment;

Injustice – stigmatisation resulting from wrongly disclosed information, leading to loss or denial of, for example, employment, training or credit;

Inappropriate Treatment – unwarranted interventions by agencies into the lives of individuals or their families, for example with draconian action being taken by mental health or child protection workers based on misinterpreted/un-contextualised data; and

Ineffective Service Delivery – because, for example, individuals do not trust agencies sufficiently to provide full and accurate information as required.

Legal & Regulatory Risk – loss of any data, particularly PID data, could result in action being taken against the CCG by the Information Commissioner if it is deemed that breaches of the Data Protection Act 1998 have occurred. In addition, the Information Commissioner, as a result of changes to the Criminal Justice Act 2008, now has the power to impose fines of up to £500,00.00 upon organisations and individuals who are aware of information risks but have not taken reasonable care and appropriate steps to mitigate those risks. Any legal and regulatory action against the CCG would be publicised and highly damaging to confidence;

The NHS Care Record Guarantee – The NHS has published a ‘Guarantee’ on how it handles patient data including the duties of keeping records confidential, secure and accurate. Unauthorised access or modification of any patient data would breach such ‘guarantees’;

Human Rights Breaches – In a Landmark Judgement, the European Court of Human Rights found that in the case of I v Finland, a patients’ Right to Family Life was breached after a hospital was found not to have maintained sufficient confidentiality of ‘I’s medical records. Failures in maintaining the confidentiality of patient data could be interpreted by a Court of Law as a breach of a patients’ Human Rights by the CCG

Staff Awareness – Staff utilising portable computing devices, portable storage devices, removable media or involved in the handling of data in transit must fully understand and comply with this Policy and all other relevant policies. Staff must understand that they must use their best endeavours to ensure that there is no loss of any portable device or loss of the CCG data in transit. Staff must understand that they may be liable for any such loss, and that any breaches of this or any other policy may result in disciplinary action including dismissal. Staff must also be aware that they may be held personally liable by the Information Commissioner, and could face fines of up to £500,000.00; and

Third-party Awareness – any user or third-party engaged in data handling, processing or transit on behalf of the CCG must comply with this Policy and all other relevant policies. Where third-parties do not comply with this Policy or any other relevant policy, the CCG will reserve the right to terminate all current contractual agreements with immediate effect. Third-party providers and their staff must also be aware that they may be held personally liable for any non-compliance with their statutory requirements by the Information Commissioner and could face fines of up to £500,000.00

9 Specific Policy Requirements

9.1 Overseas Use

Staff will not be permitted to take any laptops or other portable devices overseas (due to the risk of loss or theft or confiscation by a ‘foreign’ police force or customs department).
Where staff believe that they have a need to take any portable device or media overseas, it will be necessary to apply for a Policy waiver dispensation via the Policy Waiver Procedure.

9.2 Configuration Management

All laptops and portable storage devices used for the CCG business or holding the CCG data should be uniquely identified and registered in the CCG configuration management system.

Removable media that have been approved for use within the CCG must be uniquely identifiable and managed with overall configuration management.

Responsibility for the security of the CCG laptops and other portable devices should be assigned to the individual users and tracked alongside the employment status of such individuals.

9.3 Staff Roles & Responsibilities

The CCG Governance and Governance and Risk Manager will take overall responsibility for the management of the laptop and other portable devices portfolio.

The CCG Governance and Governance and Risk Manager shall review on a regular basis review the Laptop portfolio to ensure that it continues to meet the requirements of this Policy.

Line Managers, in collaboration with the Governance and Governance and Risk Manager are responsible for the day to day management and oversight of removable media used within their work areas to ensure full compliance with this Policy.

Line Managers are responsible for the secure storage of all unallocated removable media and its related control documentation as required by this Policy.

9.4 Staff Training

Users of laptops must be given appropriate training and instruction in the use of the laptop and its security functionality. This should include their responsibility for safeguarding the laptop and their obligation to comply with this Policy and other relevant policies.

User & Password Management

The creation and use of generic user accounts on laptops will not be permitted.

Each user account will be owned by a specific member of staff who is both permitted and authorised to use their account.

Each user account will be protected by an appropriate password, the password being a minimum of 8 characters long and requiring a combination of alphanumeric characters.

Where passwords are created to allow access for the first time, the authorising system will be configured to force users to change their passwords.

Users must not write down or store their password in any form.

Users must not share their password with any other user or person.

Users will not share their account with any other user or person.
The user authorisation system will be configured to lock and bar any access to any account following three unsuccessful logon attempts.

Where an account is locked, the CCG will ensure that user access is permitted only after performing appropriate validation checks of the user’s identify and authorisation checks to establish whether the user is permitted to access such systems or devices.

9.5 Data Management

The CCG data shall not be created or loaded onto devices which are not purchased or owned by the CCG or managed by a third-party on behalf of the CCG.

Loading the CCG data onto personal portable computing and storage devices such as laptops, memory sticks, and MP3 players to name but three examples is strictly prohibited.

All confidential data copied to portable devices and media MUST be encrypted using the NHS-approved encryption product

the CCG owned Portable Storage Devices (Digital Cameras, MP3 devices, Mobile telephones, etc.) that can be used to hold digital data must not be used to transport confidential data unless it has been encrypted using the NHS approved encryption product.

Staff and contractors are not permitted to introduce or use any removable media other than those provided or explicitly approved for use by the CCG

Removable media shall only be used by staff and contractors who have an identified and documented agreed business requirement.

The use of removable media by sub-contractors and temporary workers must be risk assessed and be specifically authorised.

When the business purpose has been satisfied, the contents of the removable media must be removed from that media through a destruction method that makes recovery of the data impossible. A log recording the permanent removal of data will be maintained.

Data held on a laptop or other portable computing device should, wherever possible, be a data copy (i.e. the original data should be held on a the CCG network location).

Any data created on a laptop or other portable device that is deemed critical or essential to the CCG operations, should be transferred to a the CCG network location within 5 working days of its creation or storage. All other data should be transferred to a the CCG network location at the earliest opportunity.

All data stored on a laptop or other portable device should be kept to that which is required for its effective business use in order to minimise the risks and impacts should a breach occur. Where there is a need to download any patient records, additional authorisation will be required via the Policy Waiver Procedure.

10 Accounting & Audit

When available on any device or system, accounting functionality will be enabled. Where available, the accounting system will be configured to record and store, as a minimum, event information for:
- User logon event information including User account, date and time of logon, date and time of logoff;
- failed logon attempts including date and time of failed logon events and number of failed attempts; and
- Account lockout event details including user account locked, date and time of account lockout, and reason for account lockout (for example failed logon attempts due to incorrect password).
- All accounting information will be securely stored on a central system. Users will not be permitted access to view or modify this system in any way.

11 Configuration of Trust Equipment

All the CCG equipment will be configured to mitigate against the misappropriation of the CCG information by unauthorised parties, and the transit of unencrypted information by any individual.

Use of removal media devices (including CD, DVD and Floppy Disc Drives) will be restricted to prevent the unauthorised copying of the CCG data. Users who believe that they have a justifiable business need to copy the CCG data to removable media will require additional authorisation via the Policy Waiver Procedure.

The CCG will, when available, implement port control software to manage the connection of portable storage devices and removable media devices on the CCG equipment, in accordance with the remainder of this Policy.

12 Encryption of Portable Computing Devices

The installation and configuration of laptop security functionality, including access control, encryption and labeling should be undertaken by appropriately trained Staff.

All the CCG owned Laptops and portable computing devices including mobile phones will be encrypted using the NHS-approved encryption product.

Some exceptions to the Policy may be made for specific situations (such as laptops used in conference rooms), but only if these computers are configured so that they cannot store data locally. Users should contact the Information Governance and Governance and Risk Manager for further advice.

13 Encryption of Portable Storage Devices

The CCG will issue encrypted USB drives to staff that need to hold or transport information on a portable device.

All USB drives must be ordered through Supplies, who will only procure USB drives approved for use by the CCG. USB drives obtained via other channels may not be supported for use on the CCG systems.

Recipients of USB drives must be authorised to receive the storage device by their Manager who must approve the user to hold and transport confidential data.

Recipients of USB drives must register their drive’s serial number with the Service Desk and set their user credentials prior to saving any data to the USB drive.

The encrypted devices remain the property of the CCG and must be returned to the Contact when a staff member leaves the organisation, no longer has a business requirement to hold
or transport confidential data, or is asked to return the device to the CCG for whatever the
reason.

14 NHS Approved Encryption Product

Staff must only use the approved encryption product selected by the CCG.

The CCG will not permit the use of any other encryption products, unless there are
exceptional circumstances and the encryption product is deployed for short term tactical
reasons. Users will be required to apply for a Policy Waiver if they believe they have a valid
reason for not using the NHS Approved Encryption Product.

Staff must utilise the appropriate user help guides that will be produced by the CCG to
educate users on how to logon and register for out-of-hours support, etc.

Connection and Use of Non-Trust Portable Storage Devices and Media

Non-the CCG portable storage devices connected to the CCG equipment will operate in a
read-only function. This is to facilitate inbound sharing of information (for example, if a
visiting speaker brings a presentation or a consultant needs to share a report or document
set).

Staff members and any other party working on behalf of the CCG may not create or load
confidential data on non-the CCG devices or media.

The CCG is not able to guarantee compatibility or provide support for any non-the CCG
device or media.

15 Secure File Transfer (SFT)

The SFT is a web service designed to allow the secure transfer of data between NHS users.
The SFT is designed to replace some physical media transfers by CD, DVD, memory sticks,
etc., transported by courier. It cannot be used to provide file transfers between NHS and
non-NHS parties.

The SFT will be employed for the transfer of PID, personal and other sensitive data that are
irregular, less than 1GB in size but exceeding 20MB in size.

Any data transfers that are routine, greater than 20MB but less than 1GB in size, will be
handled using removable media.

16 Transferring Data and Information using Removable Media

Removable media should not be taken or sent off-site unless a prior agreement or instruction
exists between two or more parties. A record will be maintained of all removable media
taken or sent off-site, or brought into or received within the CCG.

Where removable media has been taken or sent off-site, active confirmation that the media
has arrived at its destination must be obtained. Similarly, where the CCG receives media
from an external source, acknowledgement of its receipt will be provided.

Where there is a requirement to pass PID data or commercial or other sensitive data or
information to a third party, the Policy requirements are:

Data flows involving PID data must be documented and approved by the Caldicott Guardian
prior to any transport;

Date approved: October 2013
There MUST be an agreed Data Sharing agreement in place between the two or more parties that the requirements outlined in this Policy will be complied with;

Authority to use the courier service must be obtained from an appropriate level of management;

Only authorised secure couriers will be used. General Post Office signed or recorded delivery will not be permitted under any circumstances;

A signature sheet will be used to capture the details of the handover/takeover of the removable media;

The data file creation will be authorised recording name/role/date/time details;

The data file will be created and the following details recorded: name/role/date/time. The disk will be ‘burned’ to appropriate the CCG media and encrypted using the NHS Approved Encryption Algorithm;

The data being transferred must be encrypted using the NHS-approved encryption application;

The password required to unlock encrypted data must not be transferred with the media, but should be sent to the data recipient using an alternative means such as NHS email, or by telephone provided the recipient is known to the individual sending the data;

The packaging used to transport the media will be sufficient to protect the contents from any physical damage that is likely to arise during transit;

The identification of the courier will be checked before handover of the media;

A telephone call will be made from the dispatching organisation to the intended recipient at the receiving organisation to notify them of the dispatch;

The nominated staff at the destination will receive the disks and sign the signature sheet;

The recipients will then immediately inform the CCG that it has received the package and that the contents are present and correct;

Where the CCG does not receive confirmation of package delivery, it will actively seek such clarification until it is satisfied that the package has indeed been delivered safely or that it has become lost or stolen;

The recipients will then verify that it is able to access the data and that it is the correct data. This verification will occur at the earliest opportunity and no more than 3 days. The recipient will also notify the CCG that it has been able to access the data and that the data is correct within 7 days of receipt;

Where the CCG does not receive confirmation of data access, it will actively seek such confirmation until it is satisfied that the data has been accessed correctly and that no further copies are required;

Once the business requirement for the use of the data has been fulfilled, the original disks will be sent back to the CCG using the same secure courier service;

A telephone call will be made from the dispatching organisation to the intended recipient at the receiving organisation to notify them of the dispatch;
The nominated staff at the destination will receive the disks and sign the signature sheet;

Where the sender does not receive confirmation of package delivery, it will actively seek such clarification until it is satisfied that the package has indeed been delivered safely or that it has become lost or stolen;

The recipient will decrypt the data with the independently dispatched ‘password’ and confirm to the sender that it is able to access the data, and that the correct original data is present; and finally

Any incidences of data being lost at any stage of transit, including possible loss within any buildings, must be immediately reported via the CCG Incident Reporting System.

Where there is transfer of non-personal or non-sensitive data or information, Routine Courier Services or Post Office Recorded Delivery may be employed. The requirements for Routine Courier Services are:

Authority to use the courier service or Post Office Recorded Delivery must be obtained from appropriate level of management;

The courier will be selected from an approved list;

A telephone call will be made from the dispatching organisation to the intended recipient at the receiving organisation to notify them of the dispatch;

The contents being dispatched will be placed in an unused sealed envelope or package;

A signature sheet will be signed by the dispatching and receiving organisations;

The sender will check with the Courier Service that the package has indeed been delivered;

Where any loss of data occurs, the CCG will conduct further enquiries commensurate with the value of the data lost or stolen; and

Where a package has been lost or stolen, the user will comply with the requirements for reporting loss or theft of equipment detailed later in this Policy.

17 Guarding Against Loss or Theft of Equipment

In order to comply with this Policy and all other relevant policies, Staff must ensure that they use their best endeavors to prevent the loss or theft of any laptop, portable device or other media.

Laptops should be carried in protective anonymous bags or cases to reduce the likelihood of theft.

When users are travelling, laptops should be kept out-of-sight and should not be left unattended unless in a relatively secure location such as the boot of a car.

Laptops must not be left unattended in car boots overnight.

Laptops must not be left unattended in public places and users must be vigilant against opportunistic theft of laptops and other portable computing devices in busy public places such as airports, train stations, hotel lobbies, exhibition halls and public transport. Users must, when using public transport, guard against leaving or storing laptops in overhead racks where they may easily be forgotten.
Laptops must not be used with removable media in places where the media could become lost or stolen.

Staff must be vigilant in ensuring that when laptops are in use, there is no possibility of information on the screen being observed by unauthorised users.

18 Reporting Loss or Theft of Equipment

In the event that a laptop or other physical device or media is lost, staff should inform their Manager immediately.

In the event that a laptop or other physical device or media is stolen, staff are expected to report the theft to the police and obtain an incident number. At the same time, staff should also inform their Manager complete with the incident number if available.

The Manager will report the loss or theft of any device immediately to the Governance and Governance and Risk Manager.

The Manager will be responsible for escalating the incident, if necessary, via the CCG Incident Reporting System.

Any member of staff who does not report immediately the loss or theft of any laptop, portable device or other relevant media may be subject to disciplinary proceedings.

For the avoidance of doubt, if any staff member is unsure whether an incident is serious enough to merit reporting via the Incident Reporting System, they must be aware that they must report the incident regardless of any doubts that may exist.

19 Dissemination

This Policy will be available via the CCG Intranet.

An approach to dissemination of this Policy has been agreed whereby all staff will be notified, by email, of the location and nature of this Policy.

20 Implementation of this Policy.

All new and existing users of laptops and those involved in physical media transfers, and transfers using the NHS SFT Service will be required to understand and comply fully with this Policy.

This Policy is, and will continue to be, supported by a framework of additional policies, technical standards, operational procedures and guidance, to ensure that information security requirements are understood and met throughout the organisation. As stated previously, these will be updated, where necessary following additional risk and gap analysis studies.

21 Advice and Guidance

Further advice and guidance via the Governance and Governance and Risk Manager.