Policy Document Control Sheet

Reference Number	POL/HI/IG/0002						
Title	**IT Security Policy**						
Version number	10.0						
Document Type	Policy	**X**	Trust Procedure		Clinical Guideline		
Approval level (Clinical Guidelines)	Local		Trust-wide	X	N/A (not a guideline)		
Original policy date	November 1998						
Reviewing Committee	Health informatics Leadership team and Informatics Strategy Sub Committee						
Approving Committee	Integrated Quality and assurance Committee						
Approval Date	May 2018						
Next review date	March 2021						
Originating Directorate & Care Group (where applicable)	Nursing						
Document Owner	Head of Data Security and Protection						
Lead Director or Associate Director	AD Health informatics						
Scope	Trust wide						
Equality Impact Assessment completed on	May 2018						
Status	Approved						
Confidentiality	NHS restricted						
Keywords	IT; Security; Policy						
Previously known as: **POL/HI/0002**							

Final approval

Chairman or Executive Sponsor's Signature	
Date Approved	23/05/2018
Name & Job title of Chairman or Executive Sponsor	Noel Scanlon, Executive Nursing Director
Approving Committee	Integrated Quality and assurance Committee
Signed master copy held at:	Corporate Records Office, Trust Headquarters, Darlington Memorial Hospital

Version Control Table

Date Ratified	Version Number	Status
November 1998	Version 1.3	Superseded
December 2001	Version 1.4	Superseded
March 2002	Version 1.4	Superseded
October 2002	Version 1.4	Superseded
January 2005	Version 1.5	Superseded
January 2006	Version 1.6	Superseded
June 07	1.7	Superseded
July 2007	1.8	Superseded
July 2008	1.9	Superseded
March 2010	2.0	Superseded
December 2010	3.0	Superseded
February 2010	4.0	Superseded
Nov 2012	5.0	Superseded
February 2013	6.0	Superseded
March 2014	7.0	Superseded
March 2015	8.0	Superseded
March 2017	9.0	Superseded
May 2018	10.0	Approved

Table of Revisions

Date	Section	Revision	Author
12/2001	All sections	Footers on all pages.	
	Section 3.1 & 3.5	Change of responsibilities	
	Section 4.1	Legislation updated	
	Section 7.4	DP Act Dates	
	Section 8	Change of Responsibilities	
	Section 8.1	Incident Classification	
	Section 10.2	DP Act Requirements	
	Section 10.3	DP Act Requirements	
	Section 11	Change of Responsibilities	
10/2002	Section 4	Job Titles	
12/2005	Most sections	Change from IM&T to Informatics Job Titles and updated to incorporate whole Trust Requirements	
01/2006	Appendices	Updated appendix list	
June 07	All	Reviewed full Policy	
July 08	All	Updated names of referenced policies	
March	All	Reviewed full Policy	

2010			
December 2010	All	Reviewed	
Nov 12	All	Reviewed	
February 2013	10.4	Addition	IG & Compliance Manager
March 2014	9.6, 9.9	Reviewed and updated	HOIG
March 2015	All	Reviewed	HOIG
May 2018	All	Full review re new Data Protection legislation	HOIG

Contents

1. Introduction

County Durham and Darlington NHS Foundation Trust (CDDFT) holds and manages considerable personal and confidential information relating to patients, the public, the Trust and its employees. Increasing reliance is placed on computers to store and manage this information and with ever-easier ways by which information can be communicated throughout the Health Community organisations and other connected networks, this information is at greater risk of incident. It is important that a consistent approach is adopted to safeguard this information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held in both electronic and manual systems. This document sets out the CDDFT policy on information security and employees responsibilities for security of information held both manually and electronically.

2. Purpose

The purpose of this policy is to protect CDDFT information assets and systems from all threats, whether internal or external, deliberate or accidental.

This policy applies to all use of any form of electronic processing and storage of information on any Trust electronic equipment. Any information not being processed by computer at the time of its inception but later transferred to electronic systems thereby becomes subject to this policy.

This policy applies to all staff of the Trust, its agents or contractors whilst involved in any way with the Trust's electronic data processing and communication systems. It also applies to staff of other NHS Trusts who use the Trust's computer systems in the course of their work.

This policy is sanctioned by the Trust Board. Any infringement will be treated as misconduct of the most serious nature. Any breach of the policy may result in disciplinary action, which can result in dismissal.

The objective of IT security is to ensure business continuity and minimise disruption by preventing and minimising the impact of security incidents, threats and attacks.

The policy is to ensure that staff is aware of and abide by all appropriate precautions against loss of availability, integrity and confidentiality of the IT systems and their data.

The policy sets out the rules governing the handling of information, which exists in any processing system under the control of the Trust. These rules are intended to ensure that the best interests of the Trust are served by making sure that all information so processed is accurate and available only to those authorised to access it. The policy also ensures that all legal requirements are complied with.

3. Scope

It is the responsibility of all employees, including temporary and contract staff, to adhere to this IT security policy.

This policy also applies to persons who, although not employed by The Trust, have authorised access to the Internet through the computers owned or managed by The Trust. This includes staff working for County Durham and Darlington NHS Services (CDD NHS Services).

Any breach of or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action in accordance with the Trusts disciplinary policy, up to and including, in appropriate circumstances, dismissal without notice.

Information takes many forms and includes data stored electronically, transmitted across networks, printed out or written on paper, sent by fax or other methods, stored on mobile media or spoken in conversation and over the telephone. Assets also include the technical, organisational and physical infrastructure that allows communication to take place.

4. Definitions

Reference - Appendix C – Health Informatics Policy – Glossary of Terms

5. Duties

Chief Executive Officer / Managing Director

Overall responsibility for the implementation of this policy lies with the Chief Executive Officer for the Trust; Managing Director CDD NHS Services, or anyone identified by them as having responsibility in this area.

To assist the Chief Executive with the discharge of these responsibilities, the Head of Data Security and Protection has been delegated the responsibility whose role is to monitor and report on the adherence of Trust staff to the policy. Further to this designated members of staff of the Trust will be allocated responsibility for the maintenance of security of individual systems, the protection of the Trust's assets and performing particular security activities as outlined in system specific security policies. Oversight of IT security implementation is one of the responsibilities of the Trust Informatics Strategy Sub Committee.

No deviation from the statutory and legal obligation of the Trust can be sanctioned whatsoever.

Any request to vary this policy must be considered by the Informatics Strategy Sub Committee and Integrated Quality Assurance Committee before authorisation. In the event of an emergency, the Chief Executive will authorise and then submit the reasons for approval to the next meeting of the Integrated Quality Assurance Committee.

Implementation of this policy is the duty of each and every employee of the Trust. Managers are responsible for implementing the policy within their business areas, and for adherence to the policy by their staff.

The enforcement of this policy is assisted by the Head of Data Security and Protection and the Integrated Quality Assurance Committee. The Head of Data Security and

Protection is empowered by Integrated Quality and Assurance Committee and the Chief Executive to make any enquiry's, along with any other appropriate officer of the Trust, as they see fit, in the interest of the implementation of this policy. The enquiries and the responses received must be reported to one of the following as soon as possible:

• The Chief Executive
• The Integrated Quality Assurance Committee (IQAC)

The Data Security and Protection Committee will review this policy and detailed procedures allied to it on an ongoing basis, at least every three years. Changes to IT procedures mentioned within this policy or related to it may be authorised by the Integrated Quality Assurance Committee. Any amendments to this policy itself, however, will require authorisation from the Trust Board.

Also refer to **Appendix D – Information Security Responsibilities**

6. Main Content of Policy

6.1 Policy Outline

It is the policy of CDDFT to ensure that:

- Information will be protected against unauthorized access
- Confidentiality of information will be assured.
- Integrity will be maintained.
- Regulatory requirements and legislation will be met.
- Business Continuity plans will be produced, maintained and tested.
- Information Security training will be available for all staff.
- All breaches of information security, actual or suspected, will be reported to and investigated by appropriately trained individuals within the Trust, and notified to the Head of Data Security and Protection.

Standards and procedures will be produced to support this policy in line with NHS requirements. Examples of these will include virus control, access control, network and where appropriate encryption.

6.2 Security Organisation

Each site within the Trust must ensure that appropriate security organization and management structures are in place to effectively manage and co-ordinate the implementation of the policy. The purpose of this section is to outline the principles for the effective information security management.

6.3 Information Security Management

The ISO 17799/27001 Information Security Management Standard identifies two essentials for the proper organisation of information security; top level management commitment and support and appointment of an individual to manage security. It is essential that all sites ensure that the process of information security management is supported at the highest levels within the organization. Without this support and

commitment an appropriate information security management system cannot be implemented.

Within CDDFT two individuals (the Head of Data Security and Protection and Head of ICT) have responsibility for overseeing the implementation of all information security framework activities and provides co-ordination between all sites. The role of the Head of Data Security and Protection is to provide direction, to manage the progress to site security initiatives and provide advice on security solutions and legislation that impact on security. This is assisted by specialists in Health Informatics with IT security responsibility.
The responsibilities of the Head of Data Security and Protection are undertaken trust wide and include:

- Supporting individuals responsible for information security
- Developing with the Data Security and Protection Committee (DSPC), the security objectives, strategy and policy for the Trust.
- Briefing the DSPC on current threats to information security within the Trust and recommend safeguards.
- Defining and putting in place with the Trust Board the scope of Data Security and Protection management.
- Undertaking risk assessments across sites.
- Recording and investigating security incidents
- Monitoring compliance with current NHS guidance and UK legislation.
- Monitoring and reporting on the state of the Health Informatics Security trust wide to the board.
- Ensuring awareness of information security is raised trust wide.
- Monitoring compliance with the Data Security and Protection Toolkit (DSPT) relevant standards and thus elements of ISO 27001.

6.4 Information Security Infrastructure

The Trust will ensure that a suitable management forum exists to provide clear direction and visible management support for security initiatives. The DSPC will provide this function. The DSPC will consist of representatives across the Trust. The responsibilities of the group will be:

- Gaining and maintaining awareness of security threats to information faced by the Trust. This information will be maintained by the Data Security and Protection team and reported on where necessary to the DSPC and ISSC.
- Recording and where appropriate investigating breaches of security that occur within the trust, maintaining a database of all such incidents and reporting them to regional/national NHS security where appropriate.
- Developing and reviewing the security policy.
- Appointing the manager responsible for co-coordinating the implementation of security within the Trust.
- Setting the scope of information security management as required by the ISO 27001 standards and adopted by the NHS providing guidance as a whole, and providing guidance on the development for specific operational areas.
- Monitoring and reviewing the status of information security within the Trust as per Department of Health Code of Practice - Security.
- Providing advice and guidance on information security issues to the trust.

Please see DSPC Terms of Reference for lists of attendees.

6.5 Security of Third Party access

Access to the Trusts information processing facilities must be controlled. Access to facilities must not be allowed until an appropriate risk assessment and resulting security measures have been implemented and an agreement signed defining the terms for access. Assessment of the risks involved in granting third party access must take into account the following areas:

a) Type of access required:
- Physical access to offices, computer rooms, filing cabinets
- Logical access to the organizations networks, databases and information systems.

b) Reasons for access:
- Hardware and software support
- Other NHS Trusts or joint ventures

c) Method of remote access is required, i.e. via NHSnet or direct access via dial in modem, NHSN Connectivity.

Arrangements for third party access to Trust processing facilities must be based on formal written contract, which contains or refers to all the security requirements to ensure compliance with the Trusts policies and standards. Contracts should include:
- General policy on Health Informatics security and asset protection
- Description of the service (s) to be made available
- Target level of service and unacceptable levels of service
- Responsibilities in terms of legal aspects, e.g. Data Protection Act, Computer Misuse Act.
- Access control agreements and authorization process for user access.
- Requirement to maintain a list of individuals authorized to use the services and what their access rights are.
- Arrangements for reporting and investigating security incidents.

6.6 Outsourcing

If the Trust is or is considering outsourcing the management and control of all or part of its information systems, networks and/or desktop environments must ensure that security requirements are addressed in a formal written contract between the parties. The contract between the parties must address:
- Responsibilities in terms of legal requirements such as Data Protection Act, Computer Misuse Act and how these will be met.
- Arrangements to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities.
- How the confidentiality, integrity and availability of the organizations assets are to be maintained and the level of security to be applied.
- Controls, both physical and logical, to be implemented to restrict access to information to authorised users only.
- Business continuity arrangements and the right of Audit.

6.7 Asset Classification and Control

This section sets out details surrounding the classification and control of assets and identifies the requirements for asset classification and control within the Trust.

Accountability and classification of information assets ensures that appropriate protection is maintained. Each asset should have a nominated owner who is responsible for ensuring the maintenance of appropriate controls. In addition, information has varying degrees of sensitivity and criticality with some items requiring additional levels of protection. To ensure that information receives the appropriate level of classification based on its individual level of sensitivity and criticality it is important that a classification system is employed to define and communicate these levels.

6.8 Accountability for Assets

The Trust must have in place an inventory of all major assets. The inventory must clearly identify each asset, its ownership and current location. The asset register must include all major information, software, hard ware and service items to be protected.

The Trust must have in place a procedure covering the method of inventory, which outlines what information must be recorded against each asset and how and when the inventory is updated. Where the inventory is computer based, appropriate controls must be in place and a program of regular back up must be instigated.

The asset inventory must as a minimum identify; the item, its security classification, the owner of the asset, the location of the asset, the type of media (if the asset is data), the date of entry to the inventory and the date of removal. For the purposes of security, one “owner” must be appointed for each convenient logical or physical set of assets, for example: the system manager or head of department. This owner will be responsible for; identifying assets within are of responsibility, specifying in terms of security what the asset can be used for, determining who can use the asset, approving appropriate security protection for the asset and ensuring compliance with security controls.

All new equipment, software and data stores must be recorded in the asset inventory and allocated an appropriate owner.

6.9 Information Classification

Where possible the Trust should classify information assets to indicate the degree of protection required, dependent upon the sensitivity criticality of the information. Responsibility for defining the classification lies with the identified asset owner.

The Trust should have in place a procedure for information labeling and handling, which reflects the classification scheme adopted. The labeling of assets must be based on the most sensitive aspect of the asset, e.g. personal data that includes general health information may be labeled as sensitive, whereas data that includes health information relating to genetic services may be labeled as very sensitive.

For each classification of information the Trust must ensure that appropriate handling procedures have been developed to cover processing activities such as: copying, storing, transmission by manual methods such as post, transmission by electronic methods such as fax, scanning or e-mail and transmission by spoken word.
Ref: Information Risk Management Policy

6.10 Audit

The asset inventory, classification scheme and information labeling and handling procedures will be subject to regular audit to ensure compliance with this policy. Audit will ensure that:

- The asset inventory is adequate for the needs, is complete and accurate and contains all necessary detail.
- The classification scheme is suited to business needs and has considered the key measures of confidentiality, integrity and availability.
- Information labeling provides as accurate representation of the sensitivity of the asset and that labeling is appropriate.
- Information handling procedures adequately reflect the Trust's needs.

6.11 Personnel Security

This section sets out the requirements for ensuring that personnel security is addressed at the recruitment stage within the Trust. The purpose is to:

- Provide direction to other Organisations on personnel security and to ensure that appropriate personnel security structures are in place to ensure that all new staff is made aware of and have defined their information security responsibilities.
- Ensure that procedures are in place to reduce the risks of human error, theft, fraud or misuse of facilities, and to ensure that all staff is aware of the requirement to maintain the confidentiality of information and the security of information processing facilities.

The implementation of specific personnel measures (such as the Trusts disciplinary policy) to counter threats to the security of the IT systems are the responsibility of the Director of Human Resources and Organisational Development. The Director of Human Resources and Organisational Development is responsible for such measures to the Trust Board.

6.12 Including Security in Job responsibilities

Every job description must outline the employee's responsibilities with regard to Information Security. The job description must make it clear that employees are required to be aware of the Trusts policy on Information Security. Job descriptions must outline the individual's responsibilities for security in relation to their job role. This outline should draw attention to the Data Protection and Disclosure policy, Access control procedures and security incident management reporting procedures as a minimum.

Individual contracts must set out clearly that any breach of or refusal to comply with the Organisations policies is a disciplinary offence which may lead to disciplinary action, up to and including, in appropriate circumstances, dismissal without notice

All staff, as part of their contract of employment will complete a signed undertaking of confidentiality (non-disclosure).

Procedures to ensure smooth transition of responsibilities following the termination of the contracts of staff with IT responsibilities will be implemented by line managers where appropriate.

6.13 Personnel Screening and Policy

The Trust must ensure that verification checks are undertaken on all new employees, whether permanent, temporary or contractors, in line with the Trusts recruitment policies.

Where staff is employed by another organisation, such as an agency, the contract with the supplying organisation must set out the responsibilities to undertake checks to a similar level on all staff who will work within the Trust.

The performance of all staff in respect of information security, especially those who have access to sensitive information, should be reviewed on a regular basis by line management.

6.14 Confidentiality Agreements

All employee contracts must include a confidentiality and non-disclosure clause and must also include reference to the employee's legal responsibilities under the Computer Misuse Act 1990 and the Data Protection Act 2018.

Individuals who are not employed or contracted to the Trust but who have access to or may come into contact with confidential information must sign an appropriate confidentiality agreement before access is permitted. For example, this would apply to Voluntary Organisations staff that may have access to confidential information. The agreement must be signed, dated and the original returned to the Trust before access is granted.

6.15 Terms and Conditions of Employment

The terms and conditions of employment must clearly state what the employees' responsibilities are with regard to the security and confidentiality of information within the Trust.

Termination of employment procedures will include special immediate measures to ensure that staff terminating or temporarily suspended who may, for any reason, be considered to pose a risk to the security of the Trusts computer systems, are not in a position to cause harm to such a system.

6.16 Information Security Education and Training

The Trust must ensure that all employees and where appropriate third-party users are provided with appropriate training in information security as part of their induction process. The Trust must ensure that all employees are provided with the opportunity to update their information security awareness on a regular basis.

The Trust must ensure that all employees are made aware of updates to the Data Security and Protection Security policies of the Trust, and that these policies are readily available.

Induction training for staff will include an outline of the Trust's policy on IT security, their responsibility not to request or share details of patient's identifiable data with anyone unauthorised to see it, and any legal and other responsibilities.

6.17 Responding to and Reporting Security Incidents, Weaknesses and Malfunctions

The Trust must ensure that all employees are made aware of the information security incident reporting procedures and that they understand the need and process for reporting incidents.

All employees of the Trust are responsible for reporting information security related incidents, weaknesses and malfunctions as soon as possible after they are discovered.

All information security related incidents must be reported via the Trusts' Incident Management Reporting mechanisms via safeguard system.

Audit checks, by the internal audit consortium, will be carried out on systems according to a Programme agreed by the Associate Director of Health Informatics and the Trust Audit Committee.

Refer to the Security Incident Management Policy for details on how to manage and escalate an incident, also Trust Incident Management Policy.

6.18 Learning from incidents

The Trust must ensure that all reported information security incidents are logged to the Trust wide incident reporting database, to ensure that monitoring of the costs and impacts of all incidents can be carried out across the Trust. All information security related incidents will be reported to and reviewed by the Trust Data Security and Protection Committee and or Informatics Strategy Sub Committee.

6.19 Disciplinary Process

All violations of the security policy or related policies will be handled in accordance with the Trusts Disciplinary Policy.
Ref: Trust Disciplinary Policy

6.20 Physical and Environmental Security

This section sets out the requirements for the physical protection of assets associated with information processing facilities. Such assets range from manual paper records to Trust computer server rooms. These assets must be protected from unauthorised access, damage and interference, to ensure that information remains secure. The purpose of this section is to ensure that physical and environmental security is appropriately addressed, and to identify the physical and environmental security requirements within the Trust.

6.21 Secure Areas

Information processing facilities and information supporting critical or sensitive business activities must be protected by physical security perimeters and restricted to authorised personnel only. Physical security perimeters may consist of doors with key coded access, manned reception areas or swipe card controlled areas. Visitors to secure areas should be supervised at all times. Where this is not possible, unsupervised access to the areas may only be granted by a senior manager responsible for the area, and access and departure times must be recorded. Third party support services personnel should be granted access to secure areas only when required.

Offices, rooms and facilities that contain confidential information must be adequately protected. Doors and windows must be locked when unattended, and consideration given to the provision of external protection such as window screening or bars on external windows at ground level.

6.22 Equipment Security

Equipment must be physically protected from security threats and environmental hazards. Protection of equipment is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage. Equipment must be sited to minimise the risk from environmental threats, for example; theft, fire, water etc. Equipment must also be positioned in such a manner to reduce the risk of overlooking during their use.

Business critical systems must be adequately protected from power failures and power surges. Uninterruptible Power Supply (UPS) devices must be installed to support orderly close down. UPS equipment must be regularly checked and tested.

Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage. Procedures must be in place to ensure that adequate protection of cabling is considered during installation of new facilities.

Equipment must be subject to regular maintenance in accordance with manufacturer instructions. Maintenance agreements must be subject to contractual agreement, which defines the level of maintenance to be delivered, and the level of performance. Only authorised maintenance personnel are allowed to carry out repairs to IT hardware or software. Where maintenance cannot be carried out on site, where possible equipment containing sensitive or confidential data should have that data removed. Equipment may only be removed for maintenance following authorisation from the senior manager responsible for the area.

Prior to the use of any equipment outside of the Trust premises, use must be authorised by the line manager. Authorisation must be in writing and the responsible senior manager must keep a log of the equipment. The security of equipment/media used off-site, must be equivalent to that which would be used on-site.

To prevent disclosure of information, any computer equipment that has been used to process or store sensitive or confidential information must be disposed of in a secure manner. Storage devices such as hard disks must be overwritten or physically destroyed by a secure process.
Ref: Confidential Waste Policy.

The Trust will comply with all of the requirements for the NHS wide networking Code of Connection for NHS organisations.

No unlicensed software will be loaded onto a Trust computer. Only software for Trust business use will be allowed on Trust equipment.

Escrow agreements for service critical systems will be entered into, to reduce the possibility of difficulty in the event of supplier's liquidation where appropriate.

6.23 General Controls

Information left unattended on desks or displayed on computer screens is liable to unauthorised disclosure, modification or removal. The Trust should adopt a 'Clear desk and Clear Screen' policy, covering paper information, encrypted removable storage media and information displayed on computer screens. Where appropriate, paper and computer encrypted media containing sensitive information should be stored in suitable locked cabinets when not in use. Personal computers and terminals must not be left logged on when unattended.
Information of a personal confidential or commercial nature must not be saved to a computers local hard drive.

Sensitive or confidential information, when printed, must be removed from printers, photocopiers and fax machines immediately. Incoming and outgoing mail points and fax machines must be protected from unauthorised access. Where information is transferred by fax, appropriate measures must be taken to ensure that there is no accidental disclosure.
Where personal or commercial information is transferred by e-mail it must be secure and encrypted.

Ref: Safe Haven procedure
Transfer of Personal Identifiable Information Policy

6.24 Communications and Operations Management

The purpose of this section is to provide guidance in the following areas:

- The secure operation of information processing facilities.
- The minimisation of risk of system failures.
- The protection and maintenance of the integrity and availability of software, information and information processing and communication facilities.
- To ensure that information within networks and their supporting services is adequately protected.
- To ensure the Trust's assets are protected and that interruptions to business activities are minimised.
- To prevent loss, modification or misuse of information exchanged between Organisations.

6.25 Operational Procedures and Responsibilities

The Trust must ensure that all operating procedures identified within the Trust IT Security policy are documented and maintained. Changes to these documents must be authorised by management. Operating procedures must specify the detailed instructions for the execution of each job including:

- Processing and handling of information, including confidentiality requirements and information classifications.
- Work scheduling requirements.
- Instructions for handling errors or other exceptional conditions, including restricting the use of system utilities.
- Contacts for support in the event of technical or operational difficulties.
- Any instructions for handling special stationary or other special system out-puts.
- Detailed system start and recovery procedures to be followed in the event of a system failure, and
- Procedures for system housekeeping, backups, equipment maintenance, and computer room usage.

Changes to information processing facilities and systems must be controlled. The Trust must have in place formal documented change control procedures including;

- Identification and recording of significant changes and assessment of their potential impact.
- Formal approval for proposed changes.
- Communication of changes to all relevant personnel, and
- Procedures for aborting and recovering from planned unsuccessful changes.

Ref: Section 6.17 – Business Continuity Management.
Health Informatics Change Control Board procedure (CAB)

The Trust must have in place documented Incident Management Procedures to ensure an effective response to information security incidents.

The Trust should where appropriate ensure that segregation of duties is in place on all systems, to reduce the opportunities for unauthorised modification or misuse of information and information systems. The Trust must ensure where possible; development, test and operational facilities are segregated. Where possible, development and operational systems should be run on different processors, or in different domains or directories.

Ref: Section 6.16 – Systems Development & Maintenance.
IT Security Incident Management Policy
Trust Major Incident Policy

Where an external contractor is used to manage processing facilities, the Trust must ensure that an appropriate risk assessment has been undertaken and that appropriate controls have been agreed to reduce any potential exposure to damage or loss of data. These controls must be incorporated into any contract that is established.

6.26 System Planning and Acceptance

The Trust must ensure demands on system capacity are monitored and projections of future capacity requirements are made to ensure that it has adequate processing and storage facilities available. The utilisation of key system resources, such as file

servers, e-mail servers and business critical systems should be monitored so that additional capacity can be brought on-line when required.

The Trust must have in place acceptance criteria for new information systems, for upgrades and new versions. All such changes must be tested prior to acceptance.
Ref: Section 6.16 – Systems Development & Maintenance.

6.27 Protection against Malicious Software

The Trust must have in place formal controls to detect and prevent malicious software from entering the network. The controls as a minimum must include:

- A formal document requiring compliance with software licensing.
- A formal document covering the obtaining and introduction of files and software either from or via external networks.
- Installation and regular update of anti-virus detection and repair software.
- A document requiring users to check mail attachments and electronic downloads for viruses before use.
- Procedures for dealing with viruses and business continuity plans for recovering from virus attacks.

Ref: Anti-Virus Procedure
Section 6.17 – Business Continuity
E-mail and code of practice policy
Internet and Acceptable Use Policy.

6.28 Housekeeping

In order to allow the Trust to recover as quickly as possible in the event of data loss or corruption on one or more of its computer systems data essential to the business of the Trust must be backed-up. In order to achieve this there must be set procedures to cover:

- The copying of data to a medium which can then be stored in a secure place (back up).
- The retrieval of data from copy made on the medium (restore).
- The secure storage of media containing the data copies.
- The recording of details about the media and what data it stores to facilitate the easy and correct identification of a particular item of storage media when it is necessary to retrieve data from it.
- Testing the quality of the back-ups made both by log checking, verification techniques and by test retrieval of data from an item of storage media.

The Trust must ensure that all faults reported by users regarding problems with information processing or communications systems are logged, along with corrective action taken.
Where possible the Trust should investigate and implement resilient hardware solutions to minimise recovery times on critical systems. Such solutions must always be supplemented with appropriate back-up regimes to enable recovery from replicated data corruptions.

6.29 Network Management

The Trust must ensure that appropriate controls are in place to protect Trust networks from unauthorised access and to protect the security of data within the

network and connected services. Where possible the following controls should be adopted;

- Trust responsibility for the network should be separated from computer operations where appropriate.
- Responsibilities for the management of remote equipment and remote access to the network must be identified.
- Where appropriate, special controls should be implemented to protect the integrity of information passing over public networks, such as the use of encryption and digital signatures.
- The network architecture should be specifically documented, including the planned detailed settings of all hardware and software components.

Ref: Network Security Policy

6.30 Media Handling and Security

The Trust must put in place procedures for the appropriate handling and security of removable computer media such as tapes, disks, Smartphones Laptops, PDA's, USB's and printed reports etc. Procedures should include, the requirement to erase the previous contents of any re-usable media when no-longer required, formal authorisation for the removal of media from the Trust and the requirement for media to be stored in a secure manner.

The Trust must ensure that all media that is no-longer required is disposed of in a secure manner. Formal procedures for the secure disposal of media must be established.

Ref: Disposal of Confidential Waste Policy.

The handling and storage of information must be conducted in line with the Trust Data Protection Policy.

Ref: Data Protection Policy
Transfer of Personal Identifiable Information Policy

All system documentation must be stored securely, and access to system documentation must be appropriately authorised.

6.31 Exchanges of Information and Software

The Trust must ensure that the requirements for contractual agreements binding the parties to take care of exchanged information and/or software (whether electronic or manual) are established. To determine the need for a contractual, binding (legally and morally) agreement between parties, an appropriate risk assessment must be undertaken. In conjunction with the assessment results and the Information Classification guidelines, it will be apparent whether or not a formal agreement should be drawn up.

It is recommended that information classified at the higher levels should always be subject to a formal exchange agreement such as an Information sharing Protocol / Agreement. Information classified at the lower level will be subject to an informal agreement.

Dependent upon the sensitivity of the information involved and the method of exchange, the following security conditions will apply and be incorporated into the contractual agreement (unless specifically excluded due to the low security classification of the information) and/or the results of the Risk Assessment.

- Clearly defined management responsibilities and procedures for controlling and notifying sender, transmission, dispatch and receipt of both electronic and manual information.
- Definition of the minimum technical standards to be adhered to for packaging and transmission.
- A clear statement regarding the responsibilities and liabilities of each party in the event of loss of information.
- A statement of the agreed labeling system for sensitive or critical information. This will ensure that the information is readily identifiable and appropriately protected.
- Ownership and ownership rights of the information/software must be clearly stated. Responsibility for compliance (both regulatory and statutory) e.g. Data Protection Act, Software Copyright.
- Definition of the technical standards for recording and reading information/software must be clearly stated.
- Special controls adopted (e.g. cryptographic keys) must be clearly stated within the agreement.

The Trust must ensure that as far as possible, media is protected from unauthorised access, misuse or corruption during physical transport. The transport of media between sites should only be undertaken by reliable authorised couriers, should be packaged in such a way as to protect the contents from physical damage, and where appropriate special controls should be adopted where the transfer involves sensitive information, such as delivery by hand or in tamper proof containers.

Ref: Transfer of Personal Identifiable Information Policy
Third party Confidentiality Agreement Form
Data Processing Agreement Form

6.32 Security of Electronic Mail

The security of electronic mail is addressed by your Trust E-mail Policy and associated FAQ's and code of practise for email.

6.33 Security of Electronic Office Systems

The Trusts electronic information resources are vital assets, which require appropriate safeguards. Electronic office systems are vulnerable to a variety of threats, which may compromise the confidentiality, integrity and availability of information. The Trust must develop and implement appropriate procedures to address and control the business and security risks associated with these systems. Electronic office systems include, but are not limited to; Personal Digital Assistants, Desktop computers, Laptop computers, Mobile communications such as Smartphones, phones and pagers, USB memory Sticks, Voice mail facilities, Multimedia, Printers, and Photocopiers.

All of the above systems provide opportunities for confidential information to be disclosed, lost or destroyed, either accidentally or deliberately. Procedures developed should address the following areas;
Potential for disclosure of confidential information.

- Potential breaches of legislation (e.g. Data Protection Act 2018).
- Sharing of information held in the system.
- Exclusion of sensitive information from systems offering inadequate security.
- Suitability of the system for the particular business application.
- Identification of categories of user and the facilities within the system that each user may access.
- Locations from which the system may be accessed.
- Information retention and back-up.
- Business continuity arrangements.
- Potential for loss and/or destruction of information.
- Unauthorised access to or distribution of mail.

6.34 Publicly Available Systems

The Trust must have in place a formal authorisation process before information is made publicly available. Publicly available systems will include; Trust Internet based websites and Intranet notice boards. Information that is made publicly available must be adequately protected from unauthorised modification to ensure its integrity.

Information that is made publicly available must comply with the requirements of the Data Protection Act 2018 and Freedom of Information Act 2000. Information that is obtained from individuals using publicly available systems, such as websites, must be done so in accordance with the requirements of the Data Protection Act 2018. Access to publicly available systems must not allow access to the network which provides them.

6.35 Other Forms of Information Exchange

The Trust must develop and implement procedures that protect the exchange of information that use such facilities as, voice (including answering machines), , smartphones and video communications. The Trust should ensure that staff is aware of the potential risks to the confidentiality of information in using these forms of information exchange. Staff should be particularly made aware of the dangers of discussing confidential information in public areas, leaving confidential information on answering machines where it may be accessed by unauthorised persons for the transfer of confidential information.

Ref: Transfer of Personal Information Policy

6.36 Access Control

A vital element of Information Security is the control of access to information, business processes and computer facilities. Trust systems need to be strictly controlled to ensure that only those authorised can gain access and that access is defined on the basis of need. Access control is a requirement of UK legislation. Principle seven of the Data Protection Act 2018 requires Organisations to take appropriate measures to prevent the unauthorised disclosure of information, and is also a requirement of NHS policy. This section establishes the rules governing

control of access to information and information processing facilities, within the Trust and in some cases the Local Health Community.

6.37 Access Control Policy

The Trust must define an access control policy for their information systems. The policy must be based on business requirements and provide users with a clear statement of the rules and rights governing access for each user or group of users. The access control policy for the system must;

- Identify the security requirements of the individual applications,
- Identify the information related to each application,
- Detail the policies for information dissemination,
- Provide details of the relevant contractual and legislative obligations,
- Provide standard user access profiles and manage access rights which recognise all types of connections available to the system.

6.38 User Access Management

The Trust must develop formal user registration and de-registration procedures for granting access to systems. The procedure must include:

- The formal completion of an access application form, which is endorsed by the users' immediate line manager and countersigned by an authorised individual within the organisations IT department,
- The use of unique user ID's to ensure that users can be linked to and made responsible for their actions.
- Checks that the user has received appropriate authorisation from the system owner and that appropriate management approval has been obtained.
- The provision of written confirmation of access rights to the user and the requirement for users to sign to acknowledge that they understand the conditions of their access.
- Maintenance of a formal record of all users.
- Immediate removal of access rights of users who have left the organisation or change their role.
- Regular checks against the organisations personnel files, to ensure that redundant accounts do not remain live.

The Trust must ensure that the allocation and use of special privileges (the ability to override system or application controls) is restricted and controlled. The allocation of privileges must be controlled through a formal authorisation process and be dependent upon the role of the user. Special privileges, e.g. Administrator rights, must be assigned to a different user identify from those used for normal access.

Access to all critical systems within the Trust must be controlled by password. The allocation of passwords must be controlled through a formal management process, which must:

- Include the requirement of users to sign a statement binding them to keep passwords confidential.
- Ensure that users are required to maintain their own passwords and change them on a regular basis, where password changes are not enforced by the system.
- Ensure passwords are a minimum of eight alphanumeric characters and not relating to the user or the system being accessed.

- Ensure procedures for positive identification of users who forget their passwords prior to temporary ones being issued are in place.
- Ensure that users access the systems to complete their job role and comply with the Data Protection Act 2018.

The system owner must regularly review user access rights to maintain effective control over access to data and information services. Access rights for normal users should be reviewed on an annual basis and rights of privileged users on a six monthly basis.

The Trust Human Resource department should ensure that all leavers are notified to the IT department, to ensure the prompt removal of redundant user accounts.

Live data on live systems will never be used for testing and training.

This will allow:

a) testing on live systems using test patients
b) testing using extracts of live data as in my example above
c) confirmation tests following an upgrades before the system is released to users

Any live data used for demonstration purposes will require the express permission of the person concerned. Any personal data added to training or databases will be fictitious or de-identified.

6.39 User Responsibilities

All users of Organisational information processing facilities are required to follow good security practices in the selection and use of passwords. This will include:

- Keeping passwords confidential, not writing passwords down or sharing them.
- Changing their password immediately they suspect it has been compromised.
- Where systems do not enforce it, ensuring passwords are a minimum eight characters long and contain at least one non-alphabetic character.
- Not basing their password on anything that could be easily guessed by another, such as their own name, type of car, car registration, name of pets etc.
- Not recycling old passwords.
- Ensure that unattended equipment has appropriate protection.
- Leave computer terminals unattended whilst connected to the system, ensure that when a session is finished they log-out and ensure that, where available, screen saver passwords are used.
- Accessing Trust information obtained for healthcare purposes in line with their job role ensuring compliance with the Data Protection Act 2018 and other appropriate legislation.

Failure to follow good security practices may lead to disciplinary action being taken against the user. Deliberate sharing of system access passwords, is a criminal offence under the Computer Misuse Act 1990. Deliberate accessing relatives / friends / colleagues etc. information is classed as a breach of the Data Protection Act 2018.

6.40 Print screen prevention

CDDFT is entrusted with clinical, personal and private information of their patients and staff. The Trust has a legal, moral, and ethical duty to protect all clinical and personal information by ensuring the relevant security safeguards are in place.

System functionality is used to help secure sensitive information within Trust systems, the use of the print screen facility within Clinical and electronic staff based systems is no longer permitted for use, unless authorised by a senior member of staff.

This is to prevent unwarranted printouts or snapshots of information to be taken, without a legitimate reason for doing so, using the print screen button on your computers keyboard.

If the print screen function is used, your action must be fully justified prior to use, to help preserve the confidentiality of patients and staff.

Access to and the use of Trusts systems are monitored by audit trails and if the print screen function is used and not authorised, disciplinary procedures may follow.

6.41 Network and Operating System Access Control

Where the Trust employs segregation within its network, separating them into logical domains, this must be defined by the access control policy requirements and clearly defined within operating procedures.

Ref: Network Security Policy

Dial in application forms.

Access to Trust networks must be restricted to authorised users only, via a secure log on process designed to minimise the opportunity for unauthorised access. The log on process must not disclose information about the systems that would provide an unauthorised individual with assistance.

The access log on procedure must not display system or application identifiers until the process has been completed. The system must display a general warning notice to users that unauthorised access is a criminal offence, and where appropriate that information within the system is subject to the requirements of the Data Protection Act 2018.

User access to systems must be restricted only to those functions and applications that are required for the performance of their duties. Access to required systems must be explicitly defined within the authorisation process.

Where possible, unsuccessful log on attempts must be limited to three, all unsuccessful logon attempts to the system after the third attempt must be recorded. All users of the system must have a unique identifier, which is provided for their personal and sole use.

Where possible and appropriate, access times to computer systems must be restricted dependant on need. Restrictions will be based on the requirements of the individuals' job role, e.g. access to the network may be limited to the hours of 7:00 AM to 7:00 PM, Monday to Friday where there is no requirement for access outside of these hours.

Where the Trust allows remote access to its systems, this access must be subject to appropriate authentication and approval. For example, the use of cryptographic techniques, hardware tokens or a challenge/response protocol. The method of authentication must be clearly defined within remote access procedures.

6.42 Application Access Control

The Trust must ensure that access to information is only granted to those who require access in order to perform their duties. Where appropriate, the Trust must employ logical access restrictions. This should be enabled through the provision of tailored menus, which allow access only to those functions required, controlling such rights as, read, write, delete and execute.
Ref: Access Control Policy

6.43 Monitoring System Access and Use

Access and use of Trust computer systems will be monitored to detect any abuse or misuse of those systems. Monitoring activities will be undertaken by the organisations designated Health Informatics specialist staff and where appropriate the system administrator. Monitoring will occur at random times, in line with each systems specific security policy. Monitoring will include all organisational systems. Specific areas that will be monitored will include;

- Failed attempts to access systems
- Review of log on patterns for indications of abnormal use
- Allocation and activity of privileged accounts
- Tracking of selected transactions
- Use of sensitive resources
- Out of hours activity
- Inappropriate use of authorised software and IM&T equipment

The Health Informatics IT Security staff will compile monitoring reports and any unusual use of or suspected misuse of resources will be fully investigated. As part of the monitoring process, the Trusts business critical systems will also be subject to regular audit by the Internal Audit Department, who will provide reports on the state of the systems security to appropriate managers.

6.44 Mobile Computing

The Trust must ensure that mobile computing facilities are adequately protected to ensure that business information is not compromised. The Trust must ensure that all staff who use Trust mobile computing facilities have received adequate training and are aware of the increased security risks to information stored on these devices. All Trust Laptops, smartphones, USB memory sticks will be encrypted to Department of Health Standard requirements.
Ref: Secure Laptop Policy; Encryption Policy

6.45 System Development and Management

The Trust must ensure that security requirements are built into systems from the outset. Suitable controls must be in place to manage the purchase of new systems and the enhancement of existing systems, to ensure that information security is not

compromised. The purpose of this section is to ensure that security is built into all information systems within the Trust.

6.46 Security Requirements of Systems

It is the responsibility of the Head of Data Security and Protection to provide advice on the appropriate security requirements for information systems and best practice for implementation, and where necessary to liaise with partner Organisations and NHS Digital to ensure that a coherent approach has been adopted.

Individual system managers are responsible for ensuring that appropriate security requirements have been included in system specifications for new systems and system upgrades, and to ensure that all modifications to systems are logged and up to date documentation exists for their systems. The Trust must ensure that statements of business requirements for new systems, or enhancements to existing systems specify the security controls required for that system. Security requirements should be based on the classifications of information assets to be held within the system and take into account relevant legislation and guidance and an appropriate risk assessment.

The Trust Data Protection Officer and Caldicott Guardian should be notified of all new systems and changes to use, purpose or types of data held on existing systems to ensure continued compliance with the Information Commissioners Office and NHS guidelines.

6.47 Security in Application Systems

Application systems should wherever possible validate input to ensure that it is correct and appropriate, and should consider the following controls;

- Out-of-range values and invalid characters.
- Missing or incomplete data.
- Periodic review of the content of key fields or data files to confirm their validity and inspecting hard copy input documents for any unauthorised changes.
- Defining responsibilities of staff involved in the input process.
- Validation checks should be incorporated into the system in order to detect corruption of data that has been correctly input, accidentally or deliberately, during processing.

An audit facility, allowing the tracing of transactions in a system should be provided and the data owner should specify the retention period, which must be detailed in the system specific security policy. Where there is a security requirement to protect the integrity of the message content, authentication should be considered, based on an assessment of risk. System out-put should be validated to ensure the processing is correct and appropriate. This can be achieved through plausibility checks and reconciliation control counts to ensure the processing of data.

6.48 Cryptographic Controls

Where the Trust uses cryptographic controls to protect the confidentiality, authenticity or integrity of information, it must have in place a policy on its use.

6.49 Security of System Files

All modifications to the system, including changes, updates and servicing of hardware as well as software must be conducted with the security of the overall system in mind.

All software must be quality assured before live use. Where possible, system managers should test the reliability of new systems by running the new/updated system in parallel with the old. The duration of parallel system testing should be based on the potential impact of the new system failing as well as the value of the assets held within the system.

Vendor supplied software used in systems, must be maintained at a level supported by the supplier, and any decision to upgrade must take into account the security of the release. Physical or logical access should only be provided to suppliers for support purposes when necessary, and must be with management approval. All supplier activity on the system should be monitored.

6.50 Security in Developmental and Support Processes

Changes to systems must be assessed under a formal change control system. This must include an assessment of the change's impact on existing security. A record of all changes made must be maintained, and must include; the identity of the person making the change, details of the changes made, other systems affected, date and time of the change and test results.

When changes to operating systems are performed, application security should be reviewed to ensure no adverse impact on existing security.

Access to data should wherever practical be limited to anonymised / de-identified data and must be authorised by the data owner. Copies of data must retain the same levels of security and access controls as the original data. Live data must not be used for testing, training or demonstration purposes.

Testing of all upgrades to systems should be rigorous in line with the Upgrade Acceptance Testing Guidance, to ensure the integrity of the data.

All new systems implemented must meet the requirements of DSCN 2009/14 and be risk assessed and tested by the Trust in line with DSCN 2009/18.

6.51 Business Continuity Management & Disaster Recovery

The NHS and the Trust are increasingly reliant on IT services for the timely delivery of care. An emergency affecting the business critical systems of the Trust may have a significant impact on the Trusts ability to continue its operations. Procedures must be developed based upon a Risk Assessment to recover affected systems and processes to ensure continuing operations within the Organisation. This section establishes the rules on Business Continuity for the Trust. To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

6.52 Business Continuity Management / Disaster Recovery Process

The Trust must ensure a managed process is in place for the maintenance of business continuity. The process must include;

- Understanding and identifying the risks to the Trust which could result in the loss of vital systems or processes in terms of their likelihood and impact.
- Identifying and understanding the impacts which interruptions are likely to have on the business.
- Formulating and documenting business continuity plans for each of the Trusts business critical systems and processes,
- Regular testing and review of the plans and processes put in place.
- Ensuring that the business continuity plans are communicated throughout the Trust and that all affected staff is aware of what actions to take in the event of an emergency.
- Ensure that responsibility for the co-ordination of business continuity management is assigned at an appropriate level within the Trust.

6.53 Business Continuity Impact Analysis

The Trust must undertake a Business Impact Analysis (BIA) for each business critical systems. The BIA should have a defined scope and objectives, and should be sponsored by an appropriate Board Level individual. The BIA must assess the effects of disruption and loss to the Organisation in the event of an emergency. The BIA should cover the following:

- Effects of disruptions including; the loss of assets, disruption to the continuity of service and operations, violation of laws/regulations and public perception.
- Impact of disruptions such as; financial, customers and suppliers, public relations, legal, regulatory requirements, environmental, operational, personnel and other resources.
- Determine the quantitative and qualitative loss exposure including; property loss, revenue loss, human resources, morale, confidence, and corporate image.
- Production of a Business Impact Analysis Report.

The BIA must be used to define the criticality of business functions and records in order to prioritise these functions within the Trust. The BIA should also identify and determine recovery timeframes and minimum resource requirements for each identified system, including; order of recovery for business critical systems and support functions and the minimum resource requirements including; internal and external resources, owned versus non-owned resources and existing resources and additional resources required.

6.54 Writing and Implementation of Business Continuity Plans (BCP)

For the purpose of the BCP, an emergency is defined as “an event that causes disruption to the business of the Trust that may adversely affect its ability to continue normal day to day operations, which in turn may adversely affect the normal day to day operations of the NHS”. An emergency situation may be caused by events such as a fire, flood, major power outage, sabotage, terrorism and contamination.

The BCP documents the procedures to be followed to achieve timely recovery of systems that the Trust is responsible for. It specifies the types of emergencies that fall within the scope of the plan and provides detailed steps for:

- Assessing damage.
- Notifying and mobilising continuity and recovery teams.
- Initiating continuity and recovery processes and procedures.
- Recovering affected communication systems at the back up site.
- Salvaging and reconstructing affected premises.
- Restoring process and systems to the affected site, and
- Returning to normal operations.

The BCP should contain the following:

- *Storage* – A copy of the plan should be stored in a remote location from the system to which it refers, all key personnel should be aware of this location and how to access the plan in the event of an emergency.
- *Status* – The plan must clearly indicate its version number and all key personnel must be aware of the active version of the plan.
- *Communications* – The plan must clearly identify the lines of communication between the Crisis Manager and the operational units, such as service users and/or service providers. It must also clearly identify the lines of communication between the Crisis manager and other areas of the Trust which may be affected and the general public if required.

The plan must clearly identify the contacts for the provision of emergency equipment and services, which may be an external company who hold the contract for providing Disaster Recovery Services

- *Testing* – The business continuity plan must be tested on a regular basis, at least every 12 months. The results of the test must be clearly documented and any changes found necessary made as quickly as possible.
- *Updating* – The plan must be updated following each test where required, and following any major changes to the system to which it relates and re-issued.
- *Training and Awareness* – All roles and responsibilities identified within the plan must be aware of what actions they are required to take in the event of an emergency.
- *Recovery* – The plan must contain details of the recovery phase following any crisis, including tasks required and reconciliation.
- *Implementation* – The plan must clearly identify who is responsible for invoking the plan as well as identifying at least one deputy who can assume this responsibility if required.
- *General* – The plan must also indicate the frequency at which back-up copies are taken and where they are held, details of the hardware and software suppliers, details of personnel, and the location of any relevant documentation for the system.
- *Recovery Location* – Where recovery will take place away from the original site, this must be indicated in the plan.
- *Network Contingency* – Minimum network requirements, including links, software and equipment must be defined and recorded. Network recovery facilities must be tested on a regular basis.
- *Applications* – The plan should prioritise the most business critical applications to be recovered first. Account should be taken of the sequence and inter-dependencies.

6.55 Business Continuity Planning Framework

The Trust should ensure that a single framework of BCP is in place, to ensure that all plans are consistent and to identify priorities for testing and re-assessment. It is essential that when plans are changed, that other plans are reviewed for any possible impacts. The system owner is responsible for drafting and agreeing a BCP for their system, and having this plan approved by the Trusts Data Security and Protection Committee. The business continuity planning framework should provide for co-ordination of plans across the Trust, and should contain:

- An escalation procedure.
- An internal mobilisation and briefing procedure to ensure that all key staff is alerted and briefed.
- An external briefing procedure to ensure that all relevant third parties are alerted and briefed.
- Emergency procedures and fall back.
- Resumption and testing procedures.
- Training and awareness raising.
- Responsibilities.

6.56 Testing, Maintaining and Re-Assessing Business Continuity Plans

The Trust must ensure that a testing schedule is in place, which sets out which components of the plan are to be tested, when they are to be tested and who has responsibility for ensuring this testing takes place. The testing of BCPs should be monitored and the results documented. Continuity plans may be tested in a number of ways, including;

- Walk-through in differing scenarios and simulation.
- Technical recovery testing and testing of recovery to an alternative site.
- Supplier facilities and services, such as out-of hours support.
- Complete rehearsals of dealing with a major disaster.

It is the responsibility of line managers to ensure that their individual business continuity plans are regularly updated to reflect changes in service delivery. The above process will be supported by the Data Security and Protection Team.

Contingency arrangements will be reviewed by the system 'owner' at least annually. The IG team must be notified of any required changes to contingency plans.

The Head of Data Security and Protection will ensure that systems are subject to security risk assessments at least every two / three years. Risk assessments will follow a structured risk assessment methodology.

Countermeasures against the risk outlined in the assessment will be employed sensibly, efficiently and cost effectively. This will be overseen by the Associate Director of Health Informatics who will also review the countermeasures annually.

BCPs must be updated in the following circumstances; changes to key personnel, changes to contact details of personnel or systems suppliers etc., changes to location, facilities and resources, changes in legislation, changes to suppliers, changes to systems or processes and identification of new risks.

6.57 Compliance

It is the policy of the Trust to ensure that Organisations comply with applicable UK legislation and any regulatory requirements for information security. This section identifies the applicable legislation, and provides guidance on compliance with statutory requirements, the safeguarding of Trust records and the Trust IT Security Policy.

6.58 Identification of Applicable Legislation

The Trust must ensure that for each of its information systems it has identified all relevant statutory, regulatory and contractual requirements pertaining to that system. It must also ensure that individual responsibilities for meeting these requirements are also defined. These requirements should be outlined in the System Specific Security Policy for each system.

The Trust must ensure that the System Specific Security Policy addresses as a minimum, and that any use of personal identifiable information complies with the following legislation:

- The General Data Protection Regulation
- The Data Protection Act 2018
- The Freedom of information Act 2000
- The Human Rights Act 2000
- The Common Law Duty of Confidentiality.
- A Guide to Confidentiality in Health & Social Care (2013)
- Computer Misuse Act 1990

In undertaking the monitoring of its systems, the Trust must ensure that it complies with the requirements of the **Regulation of Investigatory Powers Act 2000**, and associated Lawful Business Practice Regulations, which allow the monitoring of employee communications.

The policy enforces the following UK and Legislation: the Data Protection Act (2018), the Copyright, Designs and Patents Act (1988). More recent relevant legislation includes the Regulation of Investigatory Powers Act 2000, Privacy and electronic communications (EC Directive) Regulation 2003. The policy also aims to be compliant with the existing standards, such as the ISO 27001 standards, A Guide to Confidentiality in Health & Social Care (2013) the NHS Security Manual, Caldicott Guidelines and the National Data Standards.

All employees of the Trust should be aware of and must abide by their obligations under these Acts. Any employee becoming aware of any breach of these Acts should, in the first instance, bring it to the attention of the IG Team who will make enquiry's as appropriate and bring any breach to the attention of the line manager concerned and also the Head of Data Security and Protection, CEO and the Integrated Quality and Assurance Committee.

The Head of Data Security and Protection is designated as the Trust's Data Protection Officer. They will maintain the Trust's register of applications as legally required. They will also assure the process of dealing with any Subject Access requests on behalf of the Trust and act as advisor to any staff member of the Trust on Data Protection matters.

Only legally procured and licensed software will be used by the Trust, in accordance with the terms and conditions laid out in the license agreement. Details of license software will be maintained in an asset register by IT Services who will also be responsible for carrying out regular PC audits to ensure that no unlicensed software is in use. The results of the audits are reported to the Data Security and Protection Team and the procedures for the audits are reviewed by the Internal Audit department.

6.59 Intellectual Property Rights

The **Copyright Designs and Patents Act 1988** controls the copying of software. The unauthorised copying of software is a criminal offence. The Trust must ensure that proprietary software is not used without appropriate licence. Software provided by the Trust for legitimate use must not be installed on non-organisational equipment or copied to other systems within the Trust without appropriate licence. The Trust must ensure that regular audits of installed software are conducted, and that a software asset register is maintained and regularly updated.

6.60 Safeguarding of Trust Records

The Trust must ensure that important records are protected from loss or destruction. This will include, but is not limited to, records that must be retained to meet statutory or regulatory requirements and those records required to support the Trust's essential business activities.

Guidance for the appropriate retention and storage of records within the NHS is provided within Information Governance Alliance – Records Management code of practice for Health and Social care (July 16).
Ref: Corporate Records Management Policy
Clinical Records Management Policy

6.61 Data Protection and Privacy of Personal Information

The Trust must ensure that appropriate controls are in place to protect the privacy of personal information in accordance with the requirements of the Data Protection Act 2018. All employees of the Trust must be made aware of the requirements of the legislation and in particular should be aware of sections referring to criminal offences identified within the legislation.

It is the responsibility of all Data Owners within the Trust to ensure that any proposed or current use of personal information within their work area complies with the Trusts Data Protection registered purposes.
Ref: Data Protection Policy.

Data Privacy Impact Assessments must be completed for any new, changing or developing projects that might have implications for people's privacy. These assist the Trust assess and identify any privacy concerns and address them at an early stage. The Trust has a local guidance document which must be used at the beginning of a project to implement new systems or substantive changes to services / systems.

Ref: Data Privacy Impact Assessment

6.62 Caldicott and National Data Standards

The Trust must comply with the recommendations of the 2013 Caldicott report into the use of patient-identifiable information within the NHS. Uses of personal identifiable information within the organisation must be in line with the Caldicott principles of good practice which are listed at Appendix B.
The National Data Guardian Report 2016, introduced Data Standards which must also be adhered to.

6.63 Override of Confidentiality or Patient's Express Wishes

Disclosure without consent maybe permitted in the certain circumstances; e.g. notification of communicable diseases, prevention or detection of a serious crime, i.e. terrorism, murder (under the Police and Criminal Evidence Act or Crime & Disorder Act), notification of medical condition affecting driving to DVLA (noting DVLA medical officers make the final judgment), or prevention of harm to a patient or others. Please contact DS&P department for detailed information.

Disclosure without consent is required under legislation, e.g. Road Traffic Act 1988, Prevention of Terrorism act (89) & Terrorism Act (00), Children's Act (section 47 enquiries) and where support of section 60 of the Health & Social Care act has been provided. Either as a 'class regulation' or specific authorisation from the 'Patient Information Advisory Group' or the Secretary of State for Health.

The Trust will support any member of staff who, using careful consideration and professional judgment, can satisfactorily justify any decision to disclose or withhold information against a patient's wishes, where documentary evidence can backup claims of action taken or not taken. Advice on application of legal powers and duties is available from the Data Security and Protection Team.

A patient also has the right to say no (dissent) to the Trust sharing their information as long as they fully understand the implications of not sharing regarding their on-going health care. Forms for patients who do not want their information shared are on staffnet which must be completed and sent to the Health Records department in the first instance. System Managers should be updated to ensure patient's records are not shared.

6.64 Prevention of Misuse of Information Processing Facilities

The **Computer Misuse Act 1990** is designed to protect computer systems from unauthorised access and/or modification. All users of computer systems within the Trust must be made aware of the sections of offence within the Act, and should be required to acknowledge that they have been made aware.

All computer systems within the Trust must present the user with a log-on message warning that unauthorised access is an offence under the Computer Misuse Act 1990. The deliberate unauthorised access, or damage to information systems or the data they hold is a disciplinary offence which may lead to disciplinary action in accordance with the Trusts Disciplinary Policy. Unauthorised access to systems is

also a criminal offence, and may result in legal action being taken against the perpetrator.

6.65 Collection of Evidence

The Trust must ensure that evidence to support any proposed disciplinary action against an individual is gathered in line with the Trusts disciplinary procedures. Where the Trust intends to bring civil or criminal action against an individual, it must ensure that all evidence is gathered in line with the Police and Criminal Evidence Act. Where evidence of this nature is required, the Trust must seek external advice before proceeding.

6.66 System Audit

Audits of the Trusts operational systems will be undertaken on a regular basis by Internal Auditors. The audit department will agree the scope and requirements of the audit with the Trusts management. Audit checks on systems should be limited to read-only access and must be monitored and logged. Access other than read-only, must only be allowed for isolated copies of system files, which must be erased when the audit is complete.

Access to system audit tools must be protected to prevent misuse or compromise. All use of system audit tools must be specifically authorised and a record kept of all instances of their use.

6.67 Compliance with Security Policy and Technical Compliance

The Trust must ensure that all systems are subject to regular security risk assessment and review to ensure they continue to comply with the security policy. These audits must be conducted in line with the requirements of the ISO 27001 Standard for Information Security Management. Security risk assessments should be performed within a three-year cycle, and any suggested countermeasures should be implemented without undue delay.

6.68 System procurement

IT Security Standards are mandatory and must be included in the procurement criteria for each new or replacement system. During the procurement process the Head of Data Security and Protection and Head of ICT must be consulted to ensure that the selected hardware and software will meet the agreed security requirements. The satisfaction of mandatory and desirable security requirements should be established as part of the procurement process before award of contract.

Any system procured which will contain personal data, must be capable of meeting the relevant requirements of the Data Protection Act 2018, or subsequent Data Protection legislation such as European General Data Protection Regulation (GDPR). Procurement must take into account under GDPR Accountability (Art 5) the Privacy by Design and Default. The system must be capable of processing personal information such that an individual's rights under the Act and Regulation are not compromised.

System acceptance procedures will include a section outlining the degree to which the security requirements have been met along with reasons for any which have not. They should also include test data and results and reference to the risk assessment process. The procedures will also include a test to ensure that Data Protection Subject Access can be achieved easily. Acceptance will include system security sign-off by the Head of Data Security and Protection and Head of ICT.

System Specific Security Policy for the new system should be in place before the system becomes operational.

Formal testing of the system will include attempts to cause security failures including system crashes to test data integrity following rebuild, testing of password controls and similar security measures. This test data will be kept for audit purposes.

7. Monitoring

7.1 Compliance and Effectiveness Monitoring

Compliance with this policy will be monitored as outlined in the table below.

7.2 Compliance and Effectiveness Monitoring Table

Monitoring Criterion	Response
Who will perform the monitoring?	The Corporate Records Compliance Team
What are you monitoring?	1. Compliance with the Policy for Procedural Governance Documents as follows: a) Style, format and template. b) Explanation of terms used. c) Consultation process. d) Review/approval arrangements/process. e) Associated documents. f) Supporting references. 2. Compliance with the Policy for Procedural Governance Documents as follows: a) Ratification process; and b) Review arrangements.
When will the monitoring be performed?	1. Quarterly StaffNet Policies and Procedures site audit and report. 2. Quarterly advance warning report.
How are you going to monitor?	1. Analyse the export report from StaffNet Policies and Procedures site. 2. Monitoring of Register and StaffNet with regards to

	completeness and timeframes.
What will happen if any shortfalls are identified?	Any shortfalls identified will be reported to the appropriate Document Owner and Ratification Committee.
Where will the results of the monitoring be reported?	Monitoring reports will be provided as follows: 1. and 2. Quarterly monitoring report to the appropriate Ratification Committee and relevant Lead Directors / Associate Directors.
How will the resulting action plan be progressed and monitored?	Action Plans will be developed and progressed by the Trust Secretary and monitored by the relevant Ratification Committee.
How will learning take place?	Supplementary guidance will be issued in the form of Staff Bulletins via StaffNet, the Trust's intranet. If required, the Trust Secretary will provide support/training to Document Owners.

8. Glossary of Terms

Reference - Appendix C – Health Informatics Policy – Glossary of Terms

9. Associated Documentation

This Policy is referenced from the following Trust policies and procedures:

- IT Asset Management Policy
- Disposal of Confidential Waste Policy.
- Safe Haven Procedure
- IT Change Control Board Procedure
- IT Security Incident Management Policy
- Major Incident Policy
- Anti-Virus Procedure
- Network Security Policy
- Data Protection Policy
- Transfer of Personal Identifiable Information Policy
- Access Control Policy
- Corporate Records Management Policy
- Information Risk Management Policy
- Information Governance Policy
- Internet and Acceptable Use Policy
- Laptop Security Policy
- Encryption Policy
- Clinical Records Management Policy
- Subject Access Request Procedure
- E-mail Policy; Etiquette and Code of Practice

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

- A Guide to Confidentiality in Health & Social Care (2013)
- Caldicott Principles (2016) and National Data Guardian Report (2016)
- Department of Health Code of Practice – Records Management (Nov 03)
- Department of Health Code of Practice - Security
- ISO 27001 standards
- A Guide to Confidentiality in Health & Social Care (2013)
- The NHS Security Manual

10. Appendices

Appendix A — Example Classification Scheme
Appendix B – 7 Caldicott Principles of good practice
Appendix C – Health Informatics Policy – Glossary of Terms
Appendix D – Information Security Responsibilities
Appendix E – Organisational Contact Details
Appendix F - Equality Impact Assessment

10.1 Appendix A — Example Classification Scheme

Data	Security Level	Security Description
Anonymous / No Personal Details	1	Normal
Personal details / business sensitive data	2	Confidential
Personal Health Data	3	Sensitive
Personal Health Data that includes: GUM Clinic Attendance Genetic Services Abortion Services Infertility Services Mental Health Addiction HIV Status	4	Very Sensitive

10.2 Appendix B – 7 Caldicott Principles of good practice

Uses of patient information must

- **Have a justified purpose**.

Every proposed use or transfer of person identifiable information within or from the organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

- **Not be used unless absolutely necessary**.

Person-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the flow.

- **Use only the minimum necessary person-identifiable information.**

Where the use of person identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

- **Be on a strict need-to-know basis.**

Only those individuals who need to access person-identifiable information should have access to it, and they should only have access to the information that they need to see. This may mean introducing controls and splitting information flows where one information flow is used for several purposes.

- **All users must be aware of their responsibilities.**

Action should be taken to ensure that those handling person-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect confidentiality.

- **All users must understand and comply with the law.**

Every use of person-identifiable information must be lawful.

- **The duty to share information can be as important as the duty to protect patient confidentiality.**

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

10.3 Appendix C – Health Informatics Policy – Glossary of Terms

Access Control	The prevention of unauthorised access to the resources of an IT product, programs, processes, systems, or other IT product.
Asset	Item of value to the organisation, this can include information, hardware, software and people.
Asset Owner	Individual with responsibility for the asset.
Availability	The property that information / data is available and usable on demand by an authorised individual, entity or process.
Business Continuity	The process of ensuring the organisation has the ability to continue functioning in the event of a disruption to its computer services.
Caldicott	Report into the uses of patient-identifiable information within the NHS. The report produced a number of recommendations and 26 audit areas that NHS organisation are required to implement.

Caldicott Guardian	Individual within an organisation who has responsibility for the protection and use of patient-identifiable information.
Computer Media	Methods of storing information, computer media includes; CDs, discs, tapes and also includes outputs such as paper.
Computer Misuse Act 1990	An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Copyright Designs and patents Act 1988	An Act to restate the law of copyright, with amendments; to make fresh provision as to the rights of performers and others in performances; to confer a design right in original designs; to amend the Registered Designs Act 1949; to make provision with respect to patent agents and trade mark agents; to confer patents and designs jurisdiction on certain county courts; to amend the law of patents; to make provision with respect to devices designed to circumvent copy-protection of works in electronic form; to make fresh provision penalising the fraudulent reception of transmissions; to make the fraudulent application or use of a trade mark an offence; to make provision for the benefit of the Hospital for Sick Children, Great Ormond Street, London; to enable financial assistance to be given to certain international bodies; and for connected purposes.
Cryptographic Controls	Controls for the use of encryption technologies.
Data Protection Act 2018	An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.
Electronic Communications Act 2000	An Act to make provision to facilitate the use of electronic communications and electronic data storage; to make provision about the modification of licenses granted under section 7 of the Telecommunications Act 1984; and for connected purposes.
Freedom of Information Act 2000	An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes
EU General Data Protection Regulations	A European Regulation repealing the (Directive 95/46/EC) to protect living individuals with regard to processing personal

(EU) 2016/679 27/4/16	data and the free movement of that data.
HSC 1999/053 – For the Record	Guidance on the management of NHS records within Health Authorities and Trusts.
Human Rights Act 1998	An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes.
Information Classification	Identification of the sensitivity of information.
Information Security Infrastructure	Management framework to initiate and control the implementation of information security.
Information Security Management System (ISMS)	Policies, procedures and processes that ensure that the security of any given system is maintained.
Integrity	The property that information / data has not been altered or destroyed in an unauthorised manner.
ISO 17799 Information Security Management Standard	An international standard for the management of information security adopted and mandated by the NHS Information Authority, covering the areas of confidentiality, integrity and availability of information.
IT User	Users of IT resources
Lawful Business Practice Regulations	Regulations which allow businesses to intercept communications without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the operation of their telecoms systems.
Information Governance Board	Body within the health community that ensures there is clear direction and visible management support for security initiatives across the Trust.
Local Area Network (LAN)	Physical network that provides facilities for shared information at a local level.
Local Implementation Strategy (LIS)	Provides the vehicle for the local health community to develop and agree local investments to improve the use of information and technology in line with the National Strategy for improved patient care.
Malicious Software	Software that is designed to do harm

(malware)	
Management Information Security Forum	Body within an organisation that ensures there is clear direction and visible management support for security initiatives.
Network Manager	Individual with responsibility for an organisations computer networks.
NHS Information Authority	Government department to oversee development of IM&T strategy and standards.
Regulation of Investigatory Powers Act 2000	An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected any encryption or passwords may be decrypted or accessed.
Secure Area	Area within an organisation the access to which is restricted.
Head of Data Security and Protection	Individual within the Trust with responsibility for the co-ordination of information security initiatives across the partner organisations.
System Manager	Individual with responsibility for the management and administration of a computer system.
Virus	A program which has the ability to replicate, i.e. to copy itself to other computers or disks, without being asked to do so by the computer user.
Wide Area Network (WAN)	Physical network beyond a single organisation, enabling connectivity to electronic services.

10.4 Appendix D – Information Security Responsibilities

Role	Responsibility
Chief Executive	Overall responsibility for the management and implementation of Information Security within the Trust.
Integrated Quality and Assurance Committee	Co-ordination of information security implementation across the Trust. Provision of advice/guidance/policies to partner organisations. Review and approval of common information security policies and procedures.
Informatics Strategy Sub Committee	Reviews and discussion of Health Informatics project and programme work.
Data Security and Protection Committee	Management of information security implementation within the Trust.
Caldicott Guardian	Overall responsibility for ensuring that the confidentiality of patient information is maintained within the Trust. Approval of exceptional non routine disclosures of patient information. Approval of information sharing protocols on behalf of the Trust.
Head of Data Security and Protection	To manage existing information security processes within the Trust. To work within the modernisation and reform framework to facilitate the co-ordination of information security within the local Health Community ensuring that local partner organisations meet NHS and statutory obligations for information security. To support Caldicott Guardian and to ensure that appropriate annual improvement targets are set for Health organisations. To provide advice and support on all aspects of information security and confidentiality to managers and clinicians within the Trust. To monitor compliance with Information security

	policies and procedures within the community.
Data Security and Protection Manager	To support the work of the Head of Data Security and Protection in co-coordinating and facilitating information security within the Trust as part of the modernisation and reform process.
Organisational Security Lead	Responsibility for undertaking the implementation of Information Security within the Organisation, including the implementation of policies and procedures approved by the Data Security and Protection Committee. Responsibility for the security of the Trusts IT systems and infrastructure.
Audit	Responsibility for the independent audit of the Trusts information security systems and procedures and monitoring of compliance.
Users	All users of the organisations information systems, including manual systems, are responsible for ensuring that the security of the information within those systems is maintained at all times. Users are responsible for ensuring that they are aware of the organisations policies and procedures relating to information security, and that they follow these procedures. Users are responsible for ensuring that they only make use of systems where they are authorised to, and that they use those systems in an appropriate way.
Information Asset Owners and Information Asset Administrators	All users of the organisations information systems, including manual systems, are responsible for ensuring that the security of the information within those systems is maintained at all times. Users are responsible for ensuring that they are aware of the organisations policies and procedures relating to information security, and that they follow these procedures. The roles of IAO and IAA are to ensure security of electronic data in this policy is maintained within their areas.

10.5 Appendix E – Organisational Contact Details

Contact	Number
Trust Caldicott Guardian	DMH 01325 38011
Associate Director of Health Informatics	X55969
Head of Data Security and Protection Data Protection Officer	DMH x43085
Data Security and Protection Manager Data Security and Protection Officer	Greenhouse x23645 DMH x43707
Head of ICT	DMH x 43891

10.6 Appendix F - Equality Analysis / Impact Assessment

EAIA Assessment Form v3/2013

Division/Department:	Nursing Directorate / Health Informatics
Title of policy, procedure, decision, project, function or service:	IT Security Policy
Lead person responsible:	Head of Data Security and Protection
People involved with completing this:	Data Security and Protection

Type of policy, procedure, decision, project, function or service:

Existing ☑

New/proposed ☐

Changed ☐

Date Completed:	10/05/18

Step 1 – Scoping your analysis

What is the aim of your policy, procedure, project, decision, function or service and how does it relate to equality?

To ensure Trust is compliant with legislation and staff abide by the Policy.

Who is the policy, procedure, project, decision, function or service going to benefit and how?

Full Trust staff; contractors and anyone on trust sites who wishes to dispose of confidential waste.

What barriers are there to achieving these outcomes?

None

How will you put your policy, procedure, project, decision, function or service into practice?

Full distribution Trust wide; held on staffnet policy central register

Does this policy link, align or conflict with any other policy, procedure, project, decision, function or service?

No

Step 2 – Collecting your information

What existing information / data do you have?

Follows the current policy in the trust

Who have you consulted with?

IG Committee

What are the gaps and how do you plan to collect what is missing?

None

Step 3 – What is the impact?

Using the information from Step 2 explain if there is an impact or potential for impact on staff or people in the community with characteristics protected under the Equality Act 2010?

Ethnicity or Race

None

Sex/Gender

None

Age

None

Disability

None

Religion or Belief

None

Sexual Orientation

None

Marriage and Civil Partnership (applies to workforce issues only)

None

Pregnancy and Maternity

None

Gender Reassignment

None

Other socially excluded groups or communities e.g. rural community, socially excluded, carers, areas of deprivation, low literacy skills etc.

None

Step 4 – What are the differences?

Are any groups affected in a different way to others as a result of the policy, procedure, project, decision, function or service?

No

Does your policy, procedure, project, decision, function or service discriminate against anyone with characteristics protected under the Equality Act 2010?

Yes ☐ **No** ☑

If yes, explain the justification for this. If it cannot be justified, how are you going to change it to remove or mitigate the affect?

Step 5 – Make a decision based on steps 2 - 4

If you are in a position to introduce the policy, procedure, project, decision, function or service? Clearly show how this has been decided.

Review – IG Committee; Approval ISSC and IQAC and loaded to staffnet with a Trust bulletin stating new reviewed policies available.

If you are in a position to introduce the policy, procedure, project, decision, function or service, but still have information to collect, changes to make or actions to complete to ensure all people affected have been covered please list:

How are you going to monitor this policy, procedure, project or service, how often and who will be responsible?

IG have continual assessments quarterly in place for all their policies and procedures.

Step 6 – Completion and central collation

Once completed this Equality Analysis form must be forwarded to Equality and Diversity Lead and must be attached to any documentation to which it relates.