Policy Document Control Sheet

Reference Number	POL/HI/IG/0005					
Title	Data Protection Policy					
Version number	V16.0					
Document Type	Policy	X	Trust Procedure		Clinical Guideline	
Approval level (Clinical Guidelines)	Local		Trust-wide		N/A (not a guideline)	
Original policy date	April 2004					
Reviewing Committee	Informatics Strategy Sub Committee					
Approving Committee	Integrated Quality Assurance Committee					
Approval Date	23 May 2018					
Next review date	23 May 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	March 2018					
Status	Approved					
Confidentiality	Staff in Confidence					
Keywords	Data; Protection; Disclosure; Policy					

Final approval

Chairman or Executive Sponsor's Signature	
Date Approved	23/5/2018
Name & Job title of Chairman or Executive Sponsor	Noel Scanlon, Executive Director of Nursing
Approving Committee	Integrated Quality Assurance Committee
Signed master copy held at:	Corporate Records Office, Trust Headquarters, Darlington Memorial Hospital

Previously known as: **POL/HI/0005**

Version Control Table

Date Ratified	Version Number	Status
April 2004	Version 1.0	Superseded
Dec 05	Version 2.0	Superseded
April 2006	Version 3.0	Superseded
April 2006	Version 4.0	Superseded
Jan 2007	Version 5.0	Superseded
Jun 2007	Version 6.0	Superseded
September 2008	Version 7.0	Superseded
October 2009	Version 8.0	Superseded
October 2009	Version 9.0	Superseded
January 2011	Version 10.0	Superseded
February 2011	Version 11.0	Superseded
March 2012	Version 12.0	Superseded
June 2013	Version 13.0	Superseded
May 2015	Version 14.0	Superseded
November 2015	Version 14.1	Superseded
March 2017	Version 15.0	Superseded
March 2018	Version 16.0	Approved

Table of Revisions

Date	Section	Revision	Author
22/12/05	3.6	Mobile Phone confidentiality	
Apr 06	All	Reviewed and removed mobile phone confidentiality to another policy	
Jan 07	All	Reviewed policy	
June 07	All	Reviewed policy	
September 08	All	Reviewed policy	
October 2009	Page 5	Updated section – access to third party systems. Contact point information.	
December 2010	All	Reviewed policy	
March 2012	All	Reviewed policy in line with DPA Compliance	
April 2012	All	Reviewed in line with Trust new policy formatting	
June 2013	All	Reviewed policy added appendices and sections 5 – 10 and added disclosure terms.	
March 2015	All	Reviewed policy	
November 2015	Section	Updated section 9.3 recording conversations	
March 2017	All	Full review and update	HOIG
May 2018	All	Reviewed in light of GDPR and updated	HDSP

Contents

1 Introduction

The appropriate and secure handling of personal information about living individuals is a requirement of law, this has changed in the UK from the Data Protection Act 1998 to the new European Union General Dara Protection Regulation (GDPR) and subsequent UK Data Protection Act 2018 ("DPA"). This policy incorporates confidentiality and disclosure of personal information.

This policy covers records held and processed by County Durham and Darlington NHS Foundation Trust (CDDFT). The trust is responsible for its own records under the terms of the GDPR and the DPA and it has submitted itself as a Data Controller to the Information Commissioner.

This policy covers all aspects of information within the trust, including (but not limited to):

- Patient / staff / client / service user information
- Personal information
- Organisational information

This policy also covers all aspects of handing information, (including but not limited to):

- Structured and unstructured record systems – paper and electronic
- Transmission of information – email, post and telephone
- Information systems managed by or used by the trust.

This policy covers all information systems, purchased, developed and managed by, or on behalf of, the trust and any individual working for, on behalf of, or within the organisation (including volunteers, contractors and honorary contract staff).

The NHS has in place requirements for the handling of Confidential Information, that were outlined in the Caldicott Report July 2016. Caldicott operates alongside and in addition to specific guidance and requirements of professional codes of conduct, such as the NHS Digital (NHSD) Guide to Confidentiality in Health & Social Care (2013) and Code of Practice Confidential Information (2014).

In addition to these, the Common Law, Duty of Confidence also places requirements on those who receive and use confidential information.

The Trust takes the view that the principles of confidentiality apply to all personal identifiable data, whether employee or patient, held on computer or held manually and whether communicated verbally or in writing.

The above, however, does not restrict the legitimate access of authorised staff to information, which they require to carry out their duties or to give the best possible treatment to patients or clients.

2 Purpose

CDDFT is required to meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within this Policy are based upon the European Union General Data Protection Regulation (GDPR) subsequent UK Data Protection Act 2018 ("DPA") and the Guide to Confidentiality in Health & Social Care (2013). This legislation and Department of Health and Social

Care Code (DHSC) cover the security and confidentiality of personal information within the NHS, and the European Economic Area.

The Trust also has a duty to comply with additional guidance issued by the Department of Health and Social Care, NHS Improvement, and other professional bodies.

Like all NHS Organisations, CDDFT holds and processes information about its employees, patients and other individuals for various purposes (e.g. the effective provision of healthcare services or for administrative purposes such as payroll). To comply with the DPA personal information must be collected and used fairly and lawfully, stored securely and not disclosed to unauthorised persons. The GDPR, DPA and NHS Code of Confidentiality apply to both manual and electronic data.

The GDPR and DPA mandates the use of Data Privacy Impact Assessments (DPIA's) for assessing the impact on personal information of any new systems, technologies, processes or procedures that involve the use of personal information.

Failure of the Trust, or any individual, working for, on behalf of, or within the organisation (including volunteers, contractors, and honorary contract staff) to comply with GDPR / DPA legislation could potentially result in a subsequent investigation by the Information Commissioner's Office (ICO), anfd in worst cases being fined up to EUR20,000,00 or 4% annual turnover, which ever is the greater for serious substantial data breaches.

All NHS employees have a duty of confidence to patients under common law. Furthermore statute law imposes legal obligations regarding confidentiality of personal data whether it is manually documented or collected and held within computer systems.

This policy gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, effectively and efficiently and in compliance with the law, in order to deliver the best possible care to patients.

The objective of this policy is to ensure all staff are aware and understand the legal aspects of handling personal information within the Trust in order to comply with the law.

The policy sets out the rules and legislation for 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 met.

3 Scope

It is the responsibility of each employee, including temporary and contract staff, to adhere to the Data Protection policy. 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.

4 Duties

Role	Responsibilities
Chief Executive	The Chief Executive Officer (CEO) has overall responsibility for the Data Protection Policy within the Trust. Implementation of, and compliance with this Policy is delegated to the Caldicott Guardian and designated Data Protection Officer, the Head of Data Security and Protection, and the members of the Information Governance Steering Group.
Caldicott Guardian	The Caldicott Guardian is the Trust's Medical Director. The Caldicott Guardian, by acting as the 'conscience' of the Trust, will be responsible for ensuring that: • standards for information protection are established; • issues of patient confidentiality within the Trust are implemented and monitored; • the Trust and partner organisations comply with the highest practical standards for handling personal information; • Processing and sharing of information is lawful and ethical. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.
Senior Information Risk Owner (SIRO) –	The Trust's Senior Information Risk Owner (the CEO) responsibilities include: • acting as an advocate for information risk on the Trust Board; • ensuring the Board is adequately briefed on information risk issues; • ensuring the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff; • providing assurance, through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated; • Raising the profile of any information risks within the Trust and ensuring that information security remains high on the Board agenda.
Head of Data Security and Protection and Data Protection Officer	The Head of Data Security and Protection is responsible for ensuring the Trust meets its legal obligations with regards to information and associated legislation including the Data Protection Act 2018. Deputising for the Caldicott Guardian to ensure the Trust has a managed and co-ordinated standards based approach to information governance operating within the legal and ethical frameworks. As the Data Protection Officer enacts their duties and responsibilities as per mandated legal requirements. They act as the officer who gives assurance regarding the trusts process of receiving and processing data Subject Access Requests. He/she will be the person who controls and monitors the operation of the procedures relating to data Subject Access Requests and ensures that the timescales required by the Act for responses to such requests are met.

Role	Responsibilities
Head of Health Records	The Head of Health Records is responsible, along with the Data Protection Officer, for ensuring that requests for subject access, particularly relating to medical records are dealt with promptly, correctly and within the timescales required by the GDPR and the NHS.
Senior Information Asset Owners – SIAO's and Information Asset Owners (IAOs)	Information Asset Owners will support and enable the Heads of Service/Managers to ensure the effective implementation of this policy by: • understanding the general requirements and rights of the organisation, managers and individuals under the DPA 2018. • ensuring that data protection audits are carried out in their Care Groups / Directorates on an annual basis • ensuring that in the light of these audits, any necessary changes to the processing of data are made, within the bounds of what is practicable. • ensuring any identified information risks are escalated to the Trust's risk register and managed/mitigated appropriately . It is the responsibility of IAO's, to ensure adequate and compliant procedures are developed to handle personal data and sensitive personal data. They must ensure that all personnel that they are responsible for, either working for, on behalf of, or within, CDDFT are adequately trained **on an annual basis** to ensure that up-to-date knowledge of the laws and guidelines concerning confidentiality, data protection, information security and "subject access requests" for information are applied. This includes the responsibility to ensure that new systems or procedures used for the processing of personal data are risk assessed and a Data Privacy Impact Assessment is completed. Senior Information Asset Owners may delegate the day to day running of operational procedures but may not delegate overall responsibility for the handling of personal data and sensitive personal data within their departments.
Information Asset Administrators (IAA's)	Each department will have a designated IAA. A list of these nominated personnel will be maintained as part of the Asset Register which forms part of the Trust's Records of processing activities. The day to day responsibilities for enforcing this Policy will be devolved to the Information Asset Owners, Administrators and their delegated personnel. IAA's responsibilities include: • ensuring that all users of a system under their control comply with the Data Protection Principles. • ensuring system security (be it computerised or manual system) • providing data subjects with a right to access their information as per the requirements of GDPR / DPA. • production of anonymised or pseudonymised data, where justified.
System Managers	System managers will be appointed for the major information and

Role	Responsibilities
	clinical systems throughout the Trust. Responsibility will be delegated to these officers to ensure that their systems meet the technical specifics within the DPA relating to their system. They will also be responsible for notifying the Data Protection Officer of any changes to the notification required as a result of changes to their system.
Heads of Service/ Managers	Heads of Service/Managers are responsible for ensuring that their service works within the GDPR / DPA. They will ensure that: • There are effective methods for communicating Data Protection related issues within their service • Staff attend relevant training, induction and annual mandatory updates in relation to Information Governance. • Staff are aware of and adhere to information governance policies and procedures • Incident reporting is integral to the operational activities within their areas and all incidents are reported and investigated in accordance with policy and legal requirement within 72 hours for any data breaches • Data Security and Protection issues are discussed at appropriate forums • Their IAO is kept informed of information governance issues/risks relating to their service.
All Staff includes all individuals working for, on behalf of, or within, CDDFT with access to personal information.	While you are at work you may have access to information about patients/colleagues and/or the Trust. You may come in to contact with this type of information during the course of your work or simply see, hear or read something while you are working. In these circumstances where a duty of care, either to the patient or the staff member overrides the duty of confidentiality, you must discuss the matter with your supervisor/line manager in the first instance or escalate it to the next senior manager and/or obtain advice from the Trust Caldicott Guardian or Information Governance Department. Otherwise, you must keep this information confidential. As an individual working for, on behalf of or within, the Trust you are subject to an obligation of confidentiality and must adhere to the GDPR, DPA, Caldicott Principles and NHS Information Security Procedures which form part of all employees, contractors, volunteers and honorary staff's Terms and Conditions of Employment. Professional bodies (e.g. Nursing & Midwifery Council (NMC), General Medical Council (GMC)) provide additional supplementary advice and guidance for their own disciplines. These guidelines should not conflict with this Policy or legislative requirements. All staff are responsible for: • Protecting the integrity, availability and confidentiality of Trust information; • Acting to prevent the improper use or disclosure of information; • Following the guidance as set out in this and other related

Role	Responsibilities
	documentation; • Reporting breaches of Data and Confidentiality through the Trust Incident Reporting procedure; • Ensuring the safe collection, storage, processing and disclosure of personal and confidential information; • Attending relevant training, induction and **annual mandatory training** in relation to Information Governance. This policy, and its supporting procedures and guidelines, are fully endorsed by the Trust Board through the production of these documents and their minuted approval. Any unauthorised disclosure of information by a member of staff will be considered as a disciplinary offence and will be subject to the Trust's Disciplinary Procedures.
Data Security and Protection Committee (DSPC)	It is the responsibility of the DSPC to monitor the overall implementation of the policy on behalf of the Trust.

All members of staff must ensure when accessing any of the Trust electronic or paper based personal information they do so with regard to the DPA. All information must be accurately and factually recorded in real time.

This is also the same for any systems accessed by Trust staff which are not hosted by the Trust. These third party systems must be accessed with the same regard to Trust systems.

5 Main Content of Policy

5.1 The Data Protection Act

The Trust regards the lawful and correct treatment of personal information as being of significant importance to the success of its operations and to the maintenance of confidence between the Trust and those it deals with. Therefore, the Trust will, through appropriate management and strict application of criteria and controls:

- Observe fully the conditions regarding the fair and lawful collection and use of personal information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements; ensuring:
  - the quality of information used;
  - strict checks apply to determine the length of time information is held;
  - that the rights of people about whom information is held can be fully exercised under the GDPR / DPA. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase personal information which is regarded as wrong);
  - appropriate technical and organisational security measures are implemeneted to safeguard personal information

- that personal information is not transferred abroad without an assessment and suitable safeguards in place.

The GDPR / DPA lays down regulations for the handling of personal data. For all such data it is essential to abide by the six principles plus accountablity principle which govern the use of the data.
The GDPR / DPA also dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated with respect, disposed of in a secure manner, and staff must not disclose information outside the line of duty.
In addition to these principles there are other conditions which have to be met and these are specified in the GDPR / DPA.

5.1.1 Registering with the Information Commissioners Office

It is necessary to notify the Office of the Information Commissioner when an orgainsation is processing personal information.

Copies of CDDFT registration is held by the Information Commissioners' Office and is available to the public via the ICO's website.

All databases (either electronic or manual) required under law to be registered for data protection purposes will be registered under the Trust's global notification.
Failure to register personal data or knowingly use data other than as registered will constitute an offence under the GDPR / DPA, this may result in CDDFT and/or individual employees being prosecuted and/or fined. The registration is checked regularly by the Head of Data Security and Protection to ensure that all uses and disclosure of personal data are specified within the registration.

It is essential that the Trust's registration is kept up to date, and all staff are responsible for informing the Information Governance Department of any new uses of personal identifiable data through regular reviews of their records of processing activities (Information Asset Registers).

5.1.2 Confidentiality: Guide and Code of Practice to Confidentiality in Health & Social Care (2013; 2014).& the Caldicott Committee report

In 1997 the Caldicott Committee introduced stringent guidelines in the recording, access and use of personal data within the NHS.

The Caldicott Report mandated that each NHS organisation is required to have a Caldicott Guardian; this was mandated for the NHS by Health Service Circular: HSC 1999/012.

6.1.1 5.1.3 Caldicott Guardian Registration

All NHS Trusts are required to maintain and update their Caldicott Guardian registration managed by NHS Direct (NHSD). This function is carried out by the Head of Data Security and Protection (HDSP) and copy is held locally.

5.1.4 Caldicott Principles

The Caldicott Principles were introduced by the 1987 Caldicott Report into the uses of patient-identifiable information within the NHS. This has recently been reviewed (Caldicott2) and the principles updated in April 2013. The principles it devised are to ensure that access to and use of personal information is restricted to justifiable purposes and to authorised staff.

The Caldicott Principles are:

- Justify the purpose(s).
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum amount of patient identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of his or her responsibilities.
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

Caldicott also requires the establishment of Information Sharing Protocols / Agreements where necessary and not specified in contracts, to govern the sharing or patient information between trusts and organisations. This is to ensure that each trust / organisation when receiving information will handle and protect that information in a similar way.

6.1.2 5.1.5 National Data Guardian Standards 6.1.3

In July 2016 Dame Fiona Caldicott (National Data Guardian) was asked by the government to review how personal data is protected and used within Health and social care alongside the Care Quality Commission (CQC) and to recommend: new data security standards, a method for testing compliance against these standards, and a new consent or opt-out model for data sharing in relation to patient confidential data.

There are 10 data standards that should be embedded in the health and social care system with organisations providing objective assurance about how they have complied with them.
The detailed data standards can be viewed in the appendix.

5.2 Consent

Where patients have consented to their direct healthcare being carried out, they do not have to provide their consent for their personal infromation to be processed as part of their direct treatment plan.

However, it is still very important that reasonable efforts are made to ensure that patients understand how their information is to be used to support their healthcare and that they have no objections.

(The Trust privacy notice advises who we share information with and how to withdraw).

Providing that the information is shared no more widely than absolutely necessary and that “need to know” principles are enforced. It is particularly important to check that patients understand that the information contributing to their health care, must be disclosed to other organisations or agencies.This is particularly important where the use or disclosure of information, whilst an important element of modern healthcare provision, is neither obvious nor easy to understand.

Patients entrust us with, and allow us to gather sensitive information relating to their health and other matters as part of seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. Even in circumstances where patients are unconscious or lack the competence to extend this trust the duty of confidence is not diminished. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

Information that can identify individual patients must not be used or disclosed for purposes other than their direct healthcare without either the individual's explicit consent, another lawful basis or in circumstances where there is a robust public interest or legal justification to do so.

Anonymised information is not confidential and may be disclosed in some circumstances. Guidance contained in Code of Practice and Guide to Confidentiality in Health & Social Care (2013;2014) should be followed.

5.2.1 Consent & Compliance with the DPA and Guide to Confidentiality in Health & Social Care (2013).

In order to promote a healthcare service which is open and transparent about how patient information is used and processed, the Trust has developed Privacy Notices which provide specific information about how their information will be held, collected, recorded, stored, used and shared with partner organisations for the provision of continued healthcare.

5.2.2 Patients who Prohibit the Sharing of Health Information:

5.2.2.1 for the Provision of Health Care

CDDFT works with a number of NHS organisations and independent treatment centres to provide the patient with the best possible care. In order to do this patient information may be shared securely to provide direct care in local, central and peripheral locations. If the patient chooses to prohibit this information from being disclosed to other health professionals involved in providing care, it will have an impact on the care that the Trust can deliver and that the care provided is limited and, in extremely rare circumstances, not possible to offer certain treatment options.

However, sometimes the law requires that we disclose or report certain information, but that is only done after formal authority by the Courts or by a qualified health professional. Examples include reporting a serious crime which involves murder, manslaughter, rape, treason, kidnapping, child abuse or infectious diseases that may

endanger the safety of others, such as meningitis or measles, but not HIV/AIDS.

5.2.2.2 to Relatives or Carers

Patients may wish to restrict the amount of information about their healthcare to their relatives. Patients should be encouraged to be very explicit if there is anyone that they do not want to be given information.

In the event of the patient being unable to give permission a person must be identified to act on behalf of the patient and permission obtained from him/her.

In all cases, the wishes expressed by the patient must be appropriately documented in the Medical Records.

5.2.3 Disclosure Exemptions under the Data Protection Act & Guide to Confidentiality in Health & Social Care (2013)

In certain circumstances personal information may be disclosed, however it is vital that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. Further guidance is available from the Information Governance Team and the Guide to Confidentiality in Health & Social Care (2013).

5.2.4 Disclosing Information against the Patient's Wishes without the Presence of Consent

The responsibility of whether or not information should be withheld or disclosed without the patient's consent, lies with the Senior Clinician involved at the time and cannot be delegated, however, should a situation arise where this is not possible a decision should be sought from the Caldicott Guardian.

Circumstances where the patient's right to confidentiality may be overridden are rare; examples of these situations are:

- where the patient's life may be in danger or cases when the patient may not be capable of making an appropriate decision (vital interests lawful basis)
- where there is serious danger to other people, where the rights of others may supersede those of the patient
- where there is a serious threat to the healthcare professional
- Where there is a serious threat to the community
- in other exceptional circumstances, based on professional consideration and consultation

If in doubt, staff should seek guidance, in confidence, from the Clinician/Nurse in Charge, the appropriate Senior Nurse, Manager/Directorate Manager, Caldicott Guardian or the Information Governance Department.

5.2.5 Patient & Staff Disclosure Requests Made to the Police, Social & Probation Services

Please refer to the Subject Access Requests Procedure on the trusts intranet central policy and procedure pages.

CDDFT will support any member of staff who, using careful consideration and professional judgement, can satisfactorily justify any decision to disclose or withhold information against a patient's wishes.

5.2.6 Release of Information to NHS Fraud Department

CDDFT Managers are required to provide information to the NHS Counter Fraud Service when they receive a formal written request for information relating to an investigation in to alleged fraud.

If information is agreed to be released it must still be processed in compliance with the remaining Data Protection principles.

5.2.7 Disclosure of Information about Armed Forces Personnel

Service Personnel (Members) of the UK, NATO and Commonwealth Armed Forces are entitled to full use of NHS hospitals on the same basis as civilians. In addition to the normal action taken by NHS hospitals to ensure the relatives are notified of the admission of Service patients, it is essential that the appropriate Service Authority is notified as quickly as possible in order that the necessary administrative action can be performed. Failure to inform the Service Authority may lead to the Service patient concerned being reported as absent without leave from his/her unit.

Notification to the Service Authority may be made by telephone or fax and should, where possible, include the following details in respect of the Service Personnel:

- Name and address of the reporting hospital
- Service number
- Rank, name and initials
- Unit and Address
- Date of admission
- Ward
- Next of kin details, address and telephone number
- Whether next of kin has been notified

It is important to note that duty of confidence still exists with Service Personnel and only the minimal information should be provided to the Service Authority. If specific or detailed health related information is requested, always discuss the request with the Service Personnel, and gain their consent to disclose.

Additional guidance and contact details of Service Authority Offices are included in the Department of Health: Health Service Guidance: Arrangements between the Ministry of Defence, NATO, the Commonwealth Armed Services and the NHS.

5.2.8 Non–Disclosure of Personal Information Contained in a Medical Record by a Clinician

An individual requesting access to their medical/personnel files may be refused access to parts of the information if an appropriate Clinician deems exposure to that information could cause physical or mental harm to the patient. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure should be documented.

The Trust is not required to supply copies of medical records if the individual requesting the information has:

- not provided enough support information in order for the information to belocated
- the identity of a 3rd party would be revealed if disclosure were to take place

5.2.9 Disclosure of Patient Information after Death

6.2.1

When a patient dies, information relating to that individual remains legally confidential. However, an ethical obligation to the relatives of the deceased exists and health records of the deceased are public records and governed by the provisions of the Public Records Act 1958. This permits the use and disclosure of the information within them in only limited circumstances.

The Access to Health Records Act 1990 guides access to the records of deceased only by those acting as executor of the estate or those with a claim arising from the death of the patient within one section still relevant.

This right of access is negated, however, if the individual concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive).

Additional advice and guidance relating to the disclosure of information arising due to death is available from the Legal Services Department.

5.2.10 Disclosure of Personal and Sensitive Information by Telephone

General Guidance on the Use of Telephones to Communicate Personal Information

A patient has a right to privacy so we must talk to the patient, unless we have a justified reason to speak to someone on their behalf, e.g. they have given their consent or it is in their best interests.

Avoid “alarmist” language such as ‘it’s confidential’ or jargon like ‘fast track’. If you think you may need to contact the patient by phone, ask if you can call them at work, at home or on a mobile. Ask if you can leave messages and document where necessary.

If you know the patient is unable to speak to you, or the recipient of the call tells you that they effectively act on the patient's behalf, then you can pass limited information to the recipient.

5.3 Information Sharing

5.3.1 Working in Partnership to Support Healthcare

6.3.1

In order for CDDFT to remain compliant with the GDPR, DPA, Guide to Confidentiality in Health & Social Care (2013) and Information Security Regulations, all third Party Contractors and System Suppliers must formalise, document and sign legally binding agreements / contracts.

The following are examples of documents which may be required:

- Contract between the trust and a 3rd party system suppliers
- Contract to provide healthcare information between the Trust and a private hospital
- Information sharing protocol between NHS Healthcare/Social Care Partners (Local authority)

5.3.2 Third Party Contractors & Contracts

There are a number of ways in which third parties may have access to information or other information held in systems, which will help determine how extensive the risk assessment needs to be, for example, a risk assessment for cleaning contractors will be different from that carried out for a contractor connecting to the Trust ICT network. Temporary access will also see different considerations to long-term access. It is essential that the nature and level of access is determined before the risk assessment is conducted and before the information governance elements of the contract are completed.

Contracts with external third party contractors will also be required to include statements regarding Freedom of Information Requests.

Formal contracts entered into by the Trust through the Cardea system must be reviewed by the procurement department to ensure the relevant Data Security and Protection requirements and legally binding terms and conditions are covered as necessary, prior to being signed, on behalf of the Trust. This includes the procurement (or changes) of new systems and or services.

Any other formal contracts outside the Cadea system entered into by the Trust, must be logged on Information Asset registers as the record of processing by the Senior Infromation Asset Owners and reviewed on an annual basis to ensure the relevant Data Security and Protection requirements and legally binding terms and conditions are covered as necessary, prior to being signed, on behalf of the Trust.

5.3.3 Mapping Data Flows

All flows of personal information must be registered by the care group / department information asset register and reviewed annually by the

relevant SIAO. These information asset registers are the Trusts 'Records of Processing Activities' required by law.

Any new routine flows of patient/staff information which there are queries about must be agreed by the IG department and where necessary, in conjunction with the Caldicott Guardian, before any information is transferred. Consideration must firstly be given to whether the information to be shared can be pseudonymised or anonymised. Authorisation will be considered on the content, format and method of transfer following the Trusts Transfer of personal information Policy.

It is the individual's responsibility to ensure that the IG department are informed of any proposed new/change to transfer(s) and to seek guidance where needed.

5.3.4 Information Sharing Agreements (ISA's) with other Service Providers

In order for CDDFT to effectively manage and record, the use and transfer of personal data across Healthcare Partnership boundaries the Trust has agreed to implement the use of data sharing agreements and protocols where necessary and not within contractual documents.

External organisations with a need for direct access to IT systems must comply with the Trust's dial in form.

Please note that each Information Sharing Agreement/Protocol will require authorisation from the Caldicott Guardian and Data Protection Officer prior to the infromation being shared.

All Agreements/Protocols must be registered with the IG Team and reviewed by the relevant parties, within the timeframe specified, usuall on an annual basis.

5.3.5 Procedures to ensure Safe transfer of Information

Principle 6 of the DPA legislates that; all personal data must be processed with appropriate security applied. Every member of staff is personally responsible to take precautions to ensure the security of confidential personal information both whilst it is in their possession and when it is being transferred from one person or organisation to another.

Employees must refer to the Trust's Transfer of personal information and IT Security Policies for additional specific guidance.

5.3.6 Use of Patient Information for Clinical Training

The use of information about patients is essential to the education and training of medical and other healthcare students and trainees. For most of these uses, anonymised information will be sufficient and should be used whenever practicable.

Most patients understand and accept that the education and training of medical and other healthcare students and trainees relies on their having access to information about patients.

5.3.7 Trainee Healthcare Professionals

If trainee clinicians are part of the healthcare team providing or supporting a patient's care, they can have access to the patient's personal information like other team members, unless the patient objects.

Therefore, patients must be asked to provide their consent, to allow a trainee clinician sitting in on a consultation and it is the lead clinician's responsibility to ensure that the patient is under no pressure to consent.

5.3.8 Making and Using Visual and Audio Recordings of Patients for Training

The use of visual and audio recordings of patients for training purposes is permitted.

For further information please refer to the Trust's Medical Illustration Policy

5.3.9 Use of Patient Information for System Testing

There are a number of general risks that exist whenever system testing is undertaken using live data and/or a live environment. These are:

- unauthorized access to data
- unauthorized disclosure of data
- intentional corruption of data
- unintentional corruption of data
- compromise of source system data
- loss of data
- inadequacy of data
- objections from customers

Any of the above risks can also lead to financial loss to the Trust and/or the person the information relates to. Such action could significantly damage the Trusts reputation.

Additional guidance is available from the British Standards Institute: Guidance on using Personal data to test systems

5.4 Data Privacy Impact Assessments

The GDPR / DPA mandates Data Privacy Impact Assessments (DPIAs) for all Government Departments for certain initiatives. Similarly, information risk management will be considered as part of the Government's "Gateway" reviews that monitor progress of the most important projects".

Information is available from the Trust's DPIA documents (on the IG intranet page) and must be used.

Therefore, the Trust has introduced the Data Privacy Impact Assessment procedure which includes guidance and templates for carrying out a DPIA.

The following are examples of when DPIA's are required:

- New IT System
- New Process / service
- Substantially changed Procedures
- Working in partnership with other agencies

5.5 The right of Access to Information (Subject Access Requests)

5.5.1 Information Provided to Data Subjects

The Act requires that information regarding the nature of the information collected and its uses within the Trust is communicated to the individuals to whom the data relates. This is known as the Trusts Privacy Notices informing patient how we use their information.

The Trust shall ensure that the following minimum information is communicated to the individuals to whom the data they hold relates:

- The identity of the Data Controller;
- What types of personal information is being processed
- The purpose or purposes for which personal information is processed;
- Potential disclosures of personal information and who information may be disclosed to;
- The identity of the Data Processor where relevant or whom the personal information is being disclosed to;
- The identity of the Trusts Data Protection Officer;
- How long the data wil be stored for
- The consequesnces if anything goes wrong including the Information Commissioners Officer address and contact details;
- The rights of the data subjects: (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase personal information which is regarded as wrong);
- Any further information, which is necessary to make the processing fair to include where there is any automated processing or profiling of the information.

Copies of the Trust Privacy Notices are available on the Information Governance staffnet page, and Trust Internet site.

5.5.2 Rights of the Data Subject

The Trust will ensure that personal information is handled in accordance with the rights of the Data Subject as defined by the legislation.

The GDPR / DPA requires that information be processed in accordance with the rights of the Data Subject. Data Subjects have the following rights in respect of the processing of their personal information:

- Right to be informed (Privacy Notices)
- Right of access; (Access to your medical records or staff files)
- Right to require rectification, where data is inaccurate;
- Right to erasure and destruction;
- Right to restrict / prevent processing;
- Right to portability – electronic data transferred in machine readable format;
- Right to object to automated decisions and any profiling carried out;
- Right to seek an assessment by the Information Commissioner as to whether processing is being carried out in accordance with the legislation.

The Trust may receive requests for subject access from a Data Subject or their legal representative. In all cases an access request must be dealt with within 30 days. The NHS, however, has a target of 21 days to comply with a written Subject Access Request. (Ref: Subject Access Procedure for further guidance in this area).

Some requests for information may be exempt from the GDPR / DPA. Requests from the Police can come to the Trust in in various ways:

- Through A&E
- From Wards
- Through the Trust Data Protection Officer
- Via a form (from Police)
- Through the local security management specialist

This form is held by the Police and relates to information being disclosed to the Police.

The Police form is an audit trail of information released to the Police and the reasons for the information being released should there be any subsequent query raised by the Data Subject. Normally after discussing with the Police this is a straight forward process.

The trust may also receive requests from the Coroner's Office for disclosure of information where a patient is deceased and the Coroner is investigating their death. This is the only situation where original case notes can be disclosed to the coroner's officers (Police Officers act for the coroner). However, the case notes must be copied for the Trust before they are disclosed. A form must be completed and signed by the Police.

See appendix F for flowchart as to how to respond to these access requests.

5.5.3 Data Subject Audio and Visual Recording

The trust receives requests from people to record meetings, scan's, conversations etc. There is no legislation to state this cannot happen and the management of this needs careful consideration. It is better to know that conversations are being recorded rather than they are completed covertly.

Any recording can be used to remind people of the conversations / meetings, record visually aspects of a scan etc. if people do this they must know it is their personal responsibility for that information recorded on their device.

Staff need to be aware recording is possible by people and that they must act professionally knowing their actions can be seen or heard at a later date.

Further details on best practice can be found in the Data Subject's audio and visual recording procedure.

5.6 Compliance and Assurance

5.6.1 Information Governance Assessments:

The Trust's Information Governance assessment is via the NHSD Data Security and Protection toolkit annual return which enables the Trust to measures its compliance with the information handling requirements.

5.6.2 GDPR / DPA Compliance

Compliance with the GDPR / DPA is mandatory under law and the Trust will ensure that it keeps an up to date register of all records of processing personal data.

The IG Department will carry out compliance visits throughout the Trust to be fed back to the departments, Care Group Managers, the Caldicott Guardian and the Data Security and Protection Committee.

This policy is to be made available to all individuals working for, on behalf of, or within, CDDFT staff.

5.6.3 Mandatory Training

It is mandated through NHSD Data Security and Protection Toolkit, that all NHS employees must complete IG training on an annual basis. Data Protection and Confidentiality are included as part of the training content.

The Trust will ensure that training course/presentations will support this policy. The training will ensure general awareness of the Data Protection and Caldicott Principles with more specific training for Information Asset Owners and Administrators (IAO's & IAA's).

5.6.4 Trust Induction

All new staff will attend the IG training provided at Trust Induction based on the mandatory NHSD e-learning module. A test of knowledge will be undertaken and certificates will be awarded to successful completion. Any staff requiring a further understanding will be contacted by the IG team to undertake the e-learning module individually.

5.6.5 Information Governance Mandatory Training

All staff, volunteers, contractors etc. are required to complete IG training on an annual basis. This can be undertaken via the NHSD e-learning module or by attending one of the scheduled essential training sessions throughout the year.

5.6.6 Information Governance Ad-hoc training requests

These sessions will be made available to departments on a request basis only. The session content will be developed and delivered linked to the specific departmental needs. Therefore, training content may vary dependent on recent incidents, complaints and concerns raised by patients.

5.6.7 Monitoring Compliance and Confidentiality

Compliance will be monitored through compliance to the relevant Trust IG Policies, Standard Operating Procedures, and IG audits carried out by the Information Asset Administrators / IG Officer or internal Audit.

Any incidents or potential concern will be raised in the first instance with the Care Group and Departmental Managers, prior to escalation where necessary to the Head of IG / Data Protection Officer or Caldicott Guardian. All potential breaches will be investigated in line with Trust Policy and the law.

5.6.8 Patient Experience

Patient experience will also be monitored by the IG Department by inclusion of IG questions within the Trust's patient surveys, based on promotional leaflets, posters, consent to share information, privacy and dignity, access to medical records and information security. The results will be collated and reported to the Caldicott Guardian and the Data Security and Protection Committee Members.

6.7 Non Compliance

6.7.1 Disciplinary

A breach of this policy, in your use of the Trust's information, will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:

Unlawful disclosure of Personal Data and special category (sensitive) Personal Data

Inappropriate use of Personal Data and special category (sensitive) Personal Data

Accessing patient or staff personal data including medical records in the absence of a legitimate professional relationship

Misuse of the Personal Data and special category (sensitive) Personal Data which results in any claim being made against the Trust.

6.7.2 Criminal Offences

It an offence to "knowingly or recklessly" obtain or disclose data. This makes the action of "data theft", to be a criminal act. The Criminal Justice and Immigration Act 2008 increases the penalties for this offence, the second adds a defence for reasons of journalism. This change in the law sends a very clear signal that Data Protection must be a priority and that it is completely unacceptable to be casual with people's personal information. The potential financial penalty for a substantial breach of Data is Eur20,000.000 or 4% annual turnover whichever is greater.

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 Data Protection Officer
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. 3. Assurance with the Policy for Compliance: a) contractual agreements are logged on the trusts 'records of processing' registers by Senior Information Asset Owners and are reviewed on an annual basis.
When will the monitoring be performed?	1. Quarterly StaffNet Policies and Procedures site audit and report. 2. Quarterly advance warning report. 3. Quarterly basis as per trust IRM Policy
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. 3. Checks of records of processing registers through the staffnet

	communities site.
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, 2 and 3. 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 relevant Committee 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 Data protection Officer will provide support to Document Owners.

9 Associated Documentation

This Policy refers to the following Trust policies and procedures:

- Subject Access Request Procedure
- IT Security Incident Management Policy
- Transfer of Personal Information Policy
- IT Encryption Policy
- Information Risk Policy and Procedure
- Corporate Records Management Policy
- Clinical Records Policy
- Information Quality Assurance Policy
- Data Privacy Impact Assessment Procedure

References

- Guide to Confidentiality in Health & Social Care (2013).
- EU General Data Protection Regulation
- Data protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EU Directive 2003) Regulations
- DoH Code of Practice Records Management

10 Appendices

10.1 Appendix A - Definitions of GDPR Terms

Personal Data	The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect

	information about people. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Accessible Record	(a) A health record. (b) An educational record. (c) An accessible public record. A health record is defined as; "any record which consists of information relating to the physical or mental health or condition and an individual, and has been made by or on behalf of a health professional in connection with the care of that individual".
Filing system	'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
Sensitive Person Data	The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).
Genetic Data	means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
Biometric data	means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
Data concerning health	means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
Consent	of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
Processing	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Restriction of Processing	'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
Data Subject	An individual who is the subject of personal data / information.
Data Controller	A controller determines the purposes and means of processing personal data. the GDPR places further obligations on you to ensure your contracts with processors

	comply with the GDPR. means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Data Processor	A processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
Recipient	Any person to whom personal data are disclosed.
Third Party	Any person other than; (a) the data subject, (b) the data controller or (c) any data processor or other person authorised to process data for the data controller or processor 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
Profiling	'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
Pseudonymisation	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

10.2 Appendix B - Conditions for Processing of Personal Data

Article 6 – lawfulness of processing Conditions

Processing shall be lawful only if and to the extent that at least one of the following applies:

A. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

B. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

C. processing is necessary for compliance with a legal obligation to which the controller is subject;

D. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

E. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

F. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[2]Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks

Article 7 Conditions for Consent to be lawful – indirect care

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. [1]If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. [2]Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. [1]The data subject shall have the right to withdraw his or her consent at any time. [2]The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. [3]Prior to giving consent, the data subject shall be informed thereof. [4]It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 9 Processing of Special Categories (Sensitive) personal Data

1. Processing of personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation** shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

   A. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

   B. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

   C. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

   D. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

   E. processing relates to personal data which are manifestly made public by the data subject;

   F. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

   G. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

   H. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, **medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

   I. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

   J. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

10.3 Appendix C – Data Protection Act Principles

The Act states that all Data Controllers must comply with the Data Protection Act Principles. Therefore, the Trust must adhere to the following:

Personal data shall be –

1. Personal data shall be:

    A. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    B. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    C. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    D. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    E. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

    F. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

10.4 Appendix D - Application of the Act to the Trust.

The Trust are required to hold records of processing activities as required by the Act, of the data being processed by the Trust. This includes all details required by the Information Commissioner of the purposes for which we process data, details of the information we hold and the security measures we take to ensure that the data is not damaged or wrongly disclosed.

The **record of procesing** will be reviewed regularly and amendments will be promptly made as necessary. **(this is the Trusts Infromation Asset Registers)**

The Trust will ensure that its practices relating to the holding, processing and disclosure of personal data are always in accordance with the data protection Act.

Data Subjects' right of access to data relating to them will be observed fully within the required time limit, as required by the Act and any orders made within the Act. The Trust will minimise the risk of Data Subjects having rights of action against it in the courts, but will deal promptly and efficiently with any claims that arise.

The Trust will make every effort to ensure that patients and staff are not misled as to the purpose and use to which data, obtained from them, will be put.

The Trust undertakes to ensure that data held by the Trust is adequate, relevant and not excessive in relation to the purpose for which the data is held and processed. In addition the data will be, as far as is reasonable, accurate, kept up to date and not kept for longer than necessary.

The Trust will also ensure that technical and organisational measures, as appropriate, will be taken to prevent the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

The Trust will not transfer any personal data to any country outside of the EEA, unless the recipient country has sufficient safeguards, rights and freedoms for its data subjects in relation to the processing of personal data.

The Trust will ensure that a regular program of awareness training is provided so that staff have a proper understanding of the Act and their rights and responsibilities within the Act.

The Trust will take all necessary steps to minimise the risk of civil action being taken against it by the Information Commissioner, but will deal promptly and efficiently with any such action, or threatened action. The Trust will make any necessary amendments to its procedures to prevent the same liability or risk of liability from arising in the future following such action or threatened action.

10.5 Appendix E – National Data Guardian Standards

These standards are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation. For example, GPs may want support from their system suppliers to identify and respond to cyber alerts in the first instance, and many social care organisations will want that from their Local Authority.
Commissioners should take account of the standards when commissioning services. Leaders of all health and social care organisations should commit to the following data security standards.
They should demonstrate this through audit or objective assurance, and ensure that audit enables inspection by the relevant regulator.

Leadership Obligation 1: People:
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.
Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date.
Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

10.6 Appendix F –responding to requests: Emergency situations, Police requests and Coroner

POLICE REQUEST FOR PERSONAL INFORMATION UNDER DATA PROTECTION ACT

EMERGENCY	GENERAL
Police present at A&E / Other dept. Without Police form, requesting Personal information in emergency Situation.	Police present at A&E / Other dept. with Police form fully completed
CDDFT Contact Risk Management DMH x 3141	Staff checks Police form fully signed with two signatures
CDDFT print off two copies of Police form from intranet site Information Governance: Shared documents: Data Protection	Staff release information with authority from senior in charge, hand over copies of information.
Police officer completes two forms	Staff copy information released
Staff keep1 copy of form and release Information to police who take the other Police form. (authority from senior)	Send form and copies of information to Lisa Nattrass: Trust Data Protection Officer/Head of Data Security and Protection Address below **Tamperproof envelopes**
Police return fully signed copy of Police form to Access to Health within 2 weeks. Contact details below.	

CDDFT staff send Police form and copies of information released to Access to health by secure email (scans acceptable) or in **Tamperproof envelopes** Or email form to cdda-tr.Policerequests@nhs.net

Access to Health Department
County Durham & Darlington NHS Foundation Trust
Appleton House
Lanchester Road
Durham
DH1 5XZ

Direct Line Telephone Number: 0191 3728639

Email: cdda-tr.accesstohealth@nhs.net

POLICE REQUESTING PERSONAL INFORMATION UNDER DATA PROTECTION ACT RELATING TO SERIOUS INCIDENT INVESTIGATION

Police/ requesting party present and request personal information under emergency serious incident investigation / death

Memorandum of Understanding is invoked by requesting party and CDDFT

CDDFT contact Risk management DMH x 3141

Risk management liaises with requesting party and manages release of personal information etc.

Copies of Police forms and logs of information (copies) released send to Access to health department cdda-tr.Policerequests@nhs.net by Risk Management.

Access to Health Department
County Durham & Darlington NHS Foundation Trust
Appleton House
Lanchester Road
Durham
DH1 5XZ

Direct Line Telephone Number: 0191 3728639

Email: cdda-tr.accesstohealth@nhs.net

REQUESTS FOR PERSONAL INFORMATION FROM THE CORONER

Police / Coroner representative requests personal information from the Trust.

Staff check the coroner request letter / form when presented with request.

CDDFT staff check the information requested is held, complete and available

CDDFT Staff take name, number, contact details of requesting party present.

Log what is released – Original documents need to be released

Send the letter / form to Mark Herkes / Access to Health cdda-tr.Policerequests@nhs.net

Support contacts:
Head of Health Records Access to Health / Trust Data Protection Officer
Non Clinical Risk Management

Access to Health Department
County Durham & Darlington NHS Foundation Trust
Appleton House
Lanchester Road
Durham
DH1 5XZ

Direct Line Telephone Number: 0191 3728639

Email: cdda-tr.accesstohealth@nhs.net

10.7 Appendix G - Equality Impact Assessment

Equality Analysis / Impact Assessment

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

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

Existing ☑

New/proposed ☐

Changed ☐

Date Completed: 18th May 2018

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

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 Steering Group

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 Steering group; Approval PAW 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.