Joint Policy for Cumbria Partnership Foundation Trust and North Cumbria University Hospital NHS Trust

Data Protection Policy

Reference	POL/IG/001
Version	1.0
Date Ratified	25 May 2018
Next Review Date	30 April 2021
Accountable Director	Director of Finance, Strategy and Support Services
Policy Author	Head of Information Governance

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

The Trust(s) are committed fully to compliance with the requirements of Data Protection legislation and the General Data Protection Regulations (GDPR). The GDPR and the Data Protection Act 2018 (which provides the derogations (exemptions) to the GDPR aims to balance the requirements of organisations to collect, store and manage various types of personal data in order to provide their services, with the privacy rights of the individual about whom the data is held.

TARGET AUDIENCE:

This policy applies to:

- All staff of the organisation, including temporary staff and contractors, sub-contractors;
- Any individual using information "*owned*" by the organisation(s);
- Any individual requiring access to information "owned" by the organisation(s).
- Any organisation that through a Service Level Agreement purchases IG advice and support.

TRAINING:

Data protection act training is part of the mandatory IG training – see separate training needs analysis

KEY REQUIREMENTS

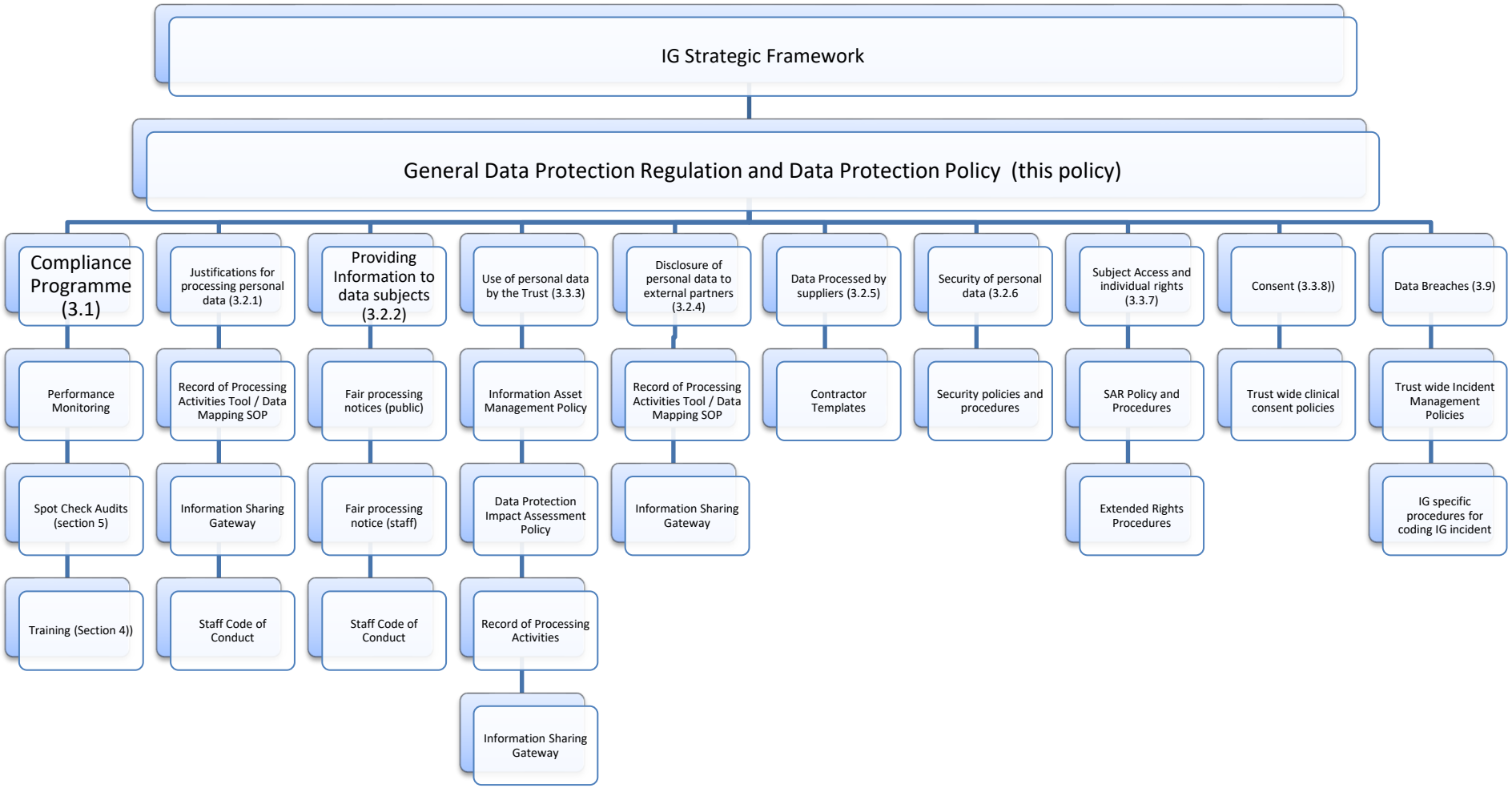
The vision of the IG department is to "***enable high quality care by facilitating the ethical, legal, effective and appropriate use of accurate and reliable information that maintains confidentiality, integrity and availability*".** This policy supports this vision.

This policy will ensure that all information used by the organisation is compliant with relevant General Data Protection Regulations and Data Protection legislation, including information systems (i.e. information assets)

This will support enhanced partnership working with other local health care organisations and wider STP footprint.

TABLE OF CONTENTS

SUMMARY FLOWCHART: (*IF APPROPRIATE) –*



1. INTRODUCTION

The Trust(s) are committed fully to compliance with the requirements of the General Data Protection Regulations and the Data Protection Act 2018 (when finalised through Parliament). The General Data Protection Regulations and Data Protection Act (DPA) 2018 aims to balance the requirements of organisations to collect, store and manage various types of personal data in order to provide their services, with the privacy rights of the individual about whom the data is held.

The GDPR and DPA legislation covers both manual and computerised records in any format, where the record contains details that can identify, directly or indirectly data on a natural person or persons. The DPA sets out principles which must be followed by those who process data; it gives rights to those whose data is being processed.

To this end, the Trust(s) endorses fully and adheres to the principles of data protection, as set out in Data Protection legislation.

- Data must be processed lawfully, fairly and in a transparent manner.
- Data must only be obtained for specified, explicit and legitimate purposes.
- Data must be adequate, relevant and limited to what is necessary for the purposes.
- Data must be accurate and up to date.
- Data must not be kept in a form that permits identification for longer than necessary for the purposes for which it is processed.
- Data must be processed in a manner which ensures appropriate security of the personal data.
- The Data Controller (the Trusts(s)) shall be responsible for, and be able to demonstrate compliance with the above principles (accountability)

2. PURPOSE

The vision of the Trusts is to "***enable high quality care by facilitating the ethical, legal, effective and appropriate use of accurate and reliable information that maintains confidentiality, integrity and availability*****".** This policy supports this vision.

3. GENERAL DATA PROTECTION REGULATIONS AND DATA PROTECTION POLICY DETAILS

The Trust will handle personal data in accordance with the Act by:

- Obtaining and processing personal data in such a way that recognises the conditions for fair processing, for compliance with a legal obligation to which the Trust is subject, and for the exercise of the Trust's statutory functions;

- Collecting and processing personal data on a 'need to know' basis, ensuring that it is fit for purpose, not excessive, is disposed of at a time appropriate for its purpose and that adequate steps are taken to ensure the accuracy and currency of data;

- Ensuring that for all personal data, appropriate technical and organisational measures are taken to prevent damage, loss or abuse;

- Ensuring that the movement of personal data is done in a lawful way – both inside and outside the organisation;

- Acknowledging the rights of individuals to whom the personal data relates and ensure that these rights may be exercised in accordance with the Act.

- Ensuring that the Information Commissioner is notified of all relevant processing and will conduct a periodic review and update of the register entries to ensure that they remain up to date;

- Ensuring that an active '*fair processing'* framework is in place, through which patients and staff are informed about the kind of purposes for which information about them is collected, and the categories of people or organisation to which such personal information may be passed. Such a framework will ensure that an individual's consent to the use of their information is informed.

Compliance via this policy is delivered through the following initiatives:

3.1 Data Protection Compliance Programme (Information Governance only)

The Information Governance Department will deliver the annual IG work plan through a compliance programme covering three main areas:

- **Process** - A set of practices and policies that make sure compliant processes are followed which are aligned with the legal requirements. This provides a structured way of managing confidential information through an established IG Strategic Framework.
- **People** - Aligning people in the organisation in terms of staff training and awareness with the end result of providing a competent staffing resource;
- **Technology** – supporting in providing the relevant tools for a competent workforce to use in line with agreed progress (management of systems, governance frameworks, best practice, audits).

Supporting this compliance programme will be a SOP (standard operating procedure) that defines the methodology and the quality criteria required for the evidence to meet the require standard with a view to a consistent approach in completing Data Security and Protection Toolkit and CQC Key Lines of Enquiry standards.

3.2 General Data Protection Regulations and Data Protection Principles

The Trust(s) will be responsible for compliance of the six privacy principles documented at Article 5 of the Regulation. The principles are as follows:

a) Lawfulness, fairness and transparency
b) Purpose Limitation

c) Data minimisation
d) Accuracy
e) Storage Limitation (retention periods)
f) Integrity and confidentiality

In addition, the Trust(s) shall be responsible for, and be able to demonstrate compliance with principles – known as the seventh principle which asserts the Trust(s) are responsible for ensuring compliance with the previous six principles and for being able to demonstrate compliance (accountability). The Trust(s) will achieve this through the Data Protection Compliance Programme summarised above (ref 3.1). A culture of accountability will be created and supported from the most senior levels as detailed in responsibilities section.

Furthermore, Data Subjects have increased rights, to:

1. Information about how their information is being processed.
2. Access to their information.
3. Rectification when information is wrong.
4. Be forgotten; when it is appropriate to do so.
5. Restrict processing.
6. Data portability.
7. Object to processing.
8. Appropriate decision-making.

In health and social care the Caldicott Principles reflect these, that when using personal identifiable data:

1. Justify the purpose(s).
2. Don't use it unless it is absolutely necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to it should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

The following indicates how the Data Protection principles will be achieved within the Trust(s):

3.2.1 Justifications for processing personal data

The Trust(s) will ensure that all collections and regular flows of personal data are documented. This will ensure compliance with the requirement to have records of processing activities (under Article 30 of the General Data Protection regulation). These records will define the legal justifications for the processing of that data.

In any processing of data identified in the records of processing activity where the Trust(s) can offer the data subject real choice and control of the use of their data for that purpose, then the processing will only be justifiable with the explicit, recorded

consent of the data subject, i.e. the publication of a photo of the data subject in a publicity brochure. Where the processing of personal data also requires the processing of special categories of personal data (also known as sensitive personal data) then in addition the relevant justification to permit the processing of such data will also be documented. The relevant retention periods for holding the information will be in line with the NHS Records Management Code of Practice.

As documented in the privacy notices the lawful conditions are documented which in the main will be under the public function condition.

3.2.2 Providing Information Notices to Data Subjects

All services will have responsibility for ensuring that they are informing data subjects of how their information is being used and in addition are expected to inform the Information Governance department of any changes and amendments so that the Team can update the Trust's Privacy Notice.

The Trust(s) will have one information notice which will be available on the Trust(s) public website.

The Trust(s) will ensure that the same processes are in place for staff and the HR department will have responsibility for ensuring that staff are informed regarding the use of their information. This will be in the form of a separate privacy notice for staff.

3.2.3 Uses of Personal data (existing and new services) by the Trust(s)

The Trust(s) will ensure that any existing uses of personal data comply with the data protection principles listed in the initial policy statement and the responsibilities of the Trust(s) set out in this policy.

In developing any new services, projects or products, the Trust(s) may be required to either collect new personal data, or use existing personal data for purposes it was not originally collected for.

In these circumstances the Trust(s) will undertake a Data Protection Impact Assessment in order to ensure that the rights of individuals under this legislation are upheld.

3.2.4 Disclosure of personal data to external parties

Any request to disclose personal data of any individual whose data is held by the Trust(s) will be considered carefully. Disclosures will only be permitted if an appropriate and necessary justification is established, in line with the requirements for lawful processing defined in data protection legislation. Any such disclosure will be recorded along with the reasons and justifications established to permit the disclosure. If a request to disclose is received, but no justification for disclosure other than consent would permit the disclosure, then disclosure will only be with the informed, explicit, recorded consent of the data subject.

Regardless of the justification for any disclosure, the data subject will be informed about the request and potential disclosure, unless to do so would prejudice any reasons for the request being made (such as prejudicing a police investigation or legal case). If the decision is taken not to inform the subject the relevant justifications as defined in legislation will be noted.

3.2.5 Data processed by suppliers on behalf of the Trust(s)

Where another organisation processes data on behalf of the Trust(s), such as a system supplier, then the Trust will ensure there is a contract in place that defines the boundaries and limitations of processing the data in terms of purposes and the requirements of the Trust to secure the personal data. This should include all the requirements put upon a 'data processor' as defined in Articles 28 & 29 of the General Data Protection Regulation.

3.2.6 Security of Personal Data

The Trusts recognise that we are privileged to have personal identifiable information and the Trust through security policies and procedures will ensure appropriate technical and organisational controls in place.

3.2.7 Subject Access and other individual rights

Any data subject of the Trust(s) may exercise their rights under General Data Protection Regulations and Data Protection legislation. The Trust will set out procedures to manage these requests in line with legislative requirements. The rights are:

- A right of access
- A right of correction (rectification)
- A right to erasure (to be forgotten)
- A right to restrict processing
- A right to portability of data
- A right to object to the processing of data
- Rights with regard to automated decision taking and profiling of data subjects

All requests to exercise rights will be responded to within timescales laid down by the legislation, either by providing the information requested, or a response of the action taken by the Trust(s).

Where any request to exercise a right is to be denied, the response will detail the justification(s) put forward by the Trust(s) in line with the exemptions and restrictions defined within the relevant data protection legislation.

3.2.8 Consent

Consent is one of the most important parts of ensuring compliance within GDPR. 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. The data subject must be able to withdraw consent at any time. The Trusts as public bodies are able to process data using the "public functions" conditions laid down in the legislation and therefore consent may not always be necessary.

3.2.9 Data Breaches

The Trust(s) will report all high risk (see definition section) data breach to the Information Commissioner's Office. Where the Trust(s) identifies that the data breach may result in a high risk to the data subject(s) then the individual will be informed.

Data Breaches will be handled in line with the overall Incident reporting policy of the Trust(s).

The legislation stipulates that infringements of the basic principles for processing are subject to the highest possible administrative fines as summarised below:

- **Level 1** – up to €10m administration fine or in the case of an undertaking, up to 2% of global turnover whichever is the higher. This Level applies to Children's Consent, unfair processing, failure of protection by design or default, joint controllers issues, failing to comply with data controller/processor responsibilities, failing to maintain records as specified, failing to cooperate with the ICO, security issues, failing to notify a breach and communicate this, lack of data protection impact assessments or consultation, failing to appoint/contract a qualified Data protection officer and interfering with their tasks.

- **Level 2** – up to €20m administration fine or in the case of an undertaking, up to 4% of global turnover whichever is the higher. This applies to non-compliance with principles, unlawful processing, failing to obtain consent, special categories of personal data processing issues, failing to provide for or comply with the data subjects rights, transfers of data and decisions on adequacy.

4. TRAINING AND SUPPORT

Employees will be made aware of their responsibilities under this policy through:

- Effective induction
- Circulation of this policy via the intranet and employee noticeboards
- Mandatory annual training.

More in-depth training will be undertaken by Information Asset Owners, Information Asset Administrators, SIRO, Caldicott Guardians etc.

5. MONITORING COMPLIANCE WITH THIS FRAMEWORK

This Information Governance Team manage compliance with this policy through the inphase Performance Management Tool as explained above under the Compliance Programme.

The Joint Information Governance Board are the Committee responsible for compliance in this regard with support from the IG Performance Group. The terms of reference of both groups are explained in the IG Strategic Framework document.

The audit and spot check document outlines the Trusts' monitoring arrangements for the IG framework arrangements within the Trust. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs. In addition, the Information Governance toolkit requirements are reviewed each year by Audit One (approved Trust auditors).

In addition the IG Performance Model in place also supports independent compliance against this framework:

- IG Performance Management Framework
- IG Performance Management monitoring procedure

The monitoring arrangements for the various areas of IG are detailed in the separate document using the ICO guide to Data Protection Audits

Aspect of compliance or effectiveness being monitored	**Monitoring method**	**Individual responsible for the monitoring**	**Frequency of the monitoring activity**	**Group / committee which will receive the findings / monitoring report**	**Group / committee / individual responsible for ensuring that the actions are completed**
Monitored via the arrangements in the document Audit and Spot Check Compliance	Various (see document)	Head of Information Governance	Various (see separate document	See governance arrangements (i.e. IG Board, Clinical Governance group etc)	Director of Finance, Strategy and Support Services
Monitored on a monthly basis via Inphase	Monthly review against KPI and tasks with associated evidence in place	Head of Information Governance	Various	See Inphase / Performance section of framework.	Director of Finance, Strategy and Support Services

The process for monitoring compliance with the effectiveness of this policy is as documented in the IG work plan with associated KPIs (Key Performance Indicators) and leads in the team to take forward.

From April 2018, the Trust's IG compliance will be measured via a self-assessment process of compliance against standards set out in the Data Security and Protection Toolkit. Once it is released the Trust will utilise it to assess its IG practice in broadly the same manner as the predecessor IG Toolkit. CQC, as outlined in Safe Data, Safe Care (2016) have powers to inspect the Trust's IG as part of its inspection round. To this end the Trust must ensure that robust IG practices are in place. CQC specifically requires that medical records are accurate, fit for purpose, held securely and held confidential.

Fundamental to the success of delivering a robust IG agenda across the Trust(s) is the development of an IG aware culture. Training is provided to all staff to promote this ethos. In particular terms this means that 95% of all staff must be trained.

6. REFERENCES AND BIBLIOGRAPHY:

- A Manual for Caldicott Guardians (2017)
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- CQC Safe Data, Safe Care (2016)
- Data Protection Act 1998 (until 24/05/2018)
- Data Protection Act 2018 (from 25/05/2018)
- Environmental Information Regulations
- Freedom of Information Act 2000
- General Data Protection Regulation / pending Data Protection Act (from 25/05/2018)
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Confidentiality NHS Code of Practice (2003)
- Human Rights Act 1998
- Records Management Code of Practice for Health and Social Care (2016)
- Information Security Management Code of Practice (2007)
- Information: To Share or Not to Share (2013) (Caldicott2)
- Privacy and Electronic Communications Regulations
- Report on the Review of Patient-Identifiable Information (1997) (The Caldicott Report)
- Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3)

7. ASSOCIATED DOCUMENTATION:

See flow chart and reference on the Trust's policy page to access the relevant policy documents.

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trust, including ensuring that Trust policies comply with all legal, statutory and good practice requirements. Data

Protection compliance responsibilities have been delegated to the Executive Director of Finance, Strategy and Support Services.

8.2 Executive Director of Finance, Strategy and Support Services

The Executive Director is responsible for ensuring that the Trust has systems and policies in place to ensure data protection compliance.

8.3 Caldicott Guardian

The Caldicott Guardian role:

- Is advisory
- Is the conscience of the organisation
- Provides a focal point for patient confidentiality and information sharing issues
- Is concerned with the management of patient information.

The Caldicott Guardian is the person with overall responsibility for ensuring the Trusts have in place the appropriate security and processes to protect person identifiable data (PID). The Caldicott Guardian plays a key role in ensuring that the organisation and partner organisations abide by the highest level for standards for handling PID and adherence to the Caldicott Principles. It is the responsibility of the Caldicott Guardian to feedback any IG issues to the Executive Senior Management Team. The Caldicott Guardian (or designated individual) is a member of the Information Governance Board. The Caldicott Guardian has a responsibility to keep up to date with developments.

8.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Officer role:

- Is accountable;
- Fosters a culture for protecting and using data;
- Provides a focal point for managing information risk and incidents
- Is concerned with the management of all information assets.

The SIRO is an Executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level. The SIRO chairs the Information Governance Board. The SIRO has a responsibility to keep up to date with developments.

8.5 Designated Data Protection Officer (DPO)

The Trust's Data Protection Officer role:

- Has a level of autonomy to pursue their duties with the full support of the controller and / or processor
- The Data Protection Officer needs to be involved properly and in a timely manner in all issues which relate to the protection of personal data. The Trust / Processor shall support the Data Protection Officer in completion of the tasks required.

- The DPO has a specific relationship with the Trust(s), it also has a specific relationship with the supervisory authority (the Information Commissioner). The DPO operations as a kind of intermediary in many instances providing a single point of contact, and ensuring that any communication with the supervisory authority and the Data Controller (the Trust(s) / data processors (i.e. contractors) are clearly understood.
- The Data Protection Officer is the single point of contact for the public for any queries relating to information about any data subject.
- To inform and advise the controller or the processor and the employees who carry out tasks of their obligations
- To monitor compliance, including the assignment of responsibilities, awareness raising and training of staff and related audits
- To provide advice with regards to Data Protection Impact Assessments
- Have due regard to the risks associated with processing operations.

8.6. Information Asset Owners (IAO)

IAOs are senior / responsible individuals working in a relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information and ensure that information is fully used within the Law for the public good, and provider written input to the SRIO annually on the security and use of their assets.

An IAO will be responsible for an information asset in terms of:

- Identifying risks associated with the information asset;
- Managing and operating the asset in compliance with policies and standards; and
- Ensuring controls manage all risks appropriately.
- Approve access to the system.

8.7. Information Asset Administrators (IAAs)

Information Asset Administrators (IAAs) have responsibility for ensuring that information asset specific policies, procedures and standard operating procedures are followed by staff and recognise actual or potential security incidents, and consult their IAO on incident management. The IAAs are senior individuals and are usually head of department or with ultimate responsibility for the information asset.

8.8. Information Security Managers

The Information Security Managers are responsible for the provision and management of a high quality, customer focussed, Information Technology Security Advisory Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

8.9. Information Governance Team

The Information Governance Team provides advice and guidance on all aspects of data protection compliance.

8.10. Human Resource Department

The Human Resources Department as responsible for compliance under this policy with all matters affecting staff compliance (i.e. fair processing notice for staff).

8.11. Managers

Managers are responsible for ensuring departmental record-keeping processes and all other departmental procedures adhere to this policy and that their teams adhere to the principles within this policy. Managers must ensure:

- Staff complete training in information governance
- Ensure that data protection incidents are reported by individual and investigate where appropriate.
- Ensure processes are maintaining the rights of data subject
- Ensure any change in process has a data protection assessment completed
- Ensure that data flows are appropriately mapped.

8.12. All staff

All staff are responsible for ensuring that:

- Keep up to date with IG training.
- any personal or sensitive personal data that they hold is kept securely and only used for legitimate business of the Trust(s).
- Personal, sensitive personal data and or any other restricted data is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Reporting any near misses or incidents related to personal data, so they can be investigated and managed.

All staff are additionally responsible for:

- checking that any information that they provide to the Trust(s) in connection with their employment is accurate and up to date.
- informing the Trust(s) of any changes to information that they have provided, including but not limited to changes of address, either at the time of appointment or subsequently. The Trust(s) cannot be held responsible for any errors unless the employee has informed it of such changes.

Any member of staff, or other individuals who considers that the policy has not been followed in respect of personal data about himself or herself, should raise the matter with his or her line manager in the first instance and then to the Trust(s) Data Protection Officer.

Staff should note that unauthorised disclosure of data deemed, personal, sensitive (special category) personal, confidential and restricted under the definitions in this policy will usually be a disciplinary matter, and may be considered gross misconduct

in some cases. Therefore it is essential, if unsure, to check whether the disclosure is necessary or legally permissible by checking with the Data Protection Officer.

Staff should also follow the requirements of the Information and Cyber Security policy to ensure that all data in all formats/media is managed securely in line with it's classification under the handling guidelines.

Staff will be required to report any incident related to data via the incident management system (Ulysses) so that swift remedial and containment action can be applied.

8.13. Approving Committee Responsibilities:

The Chair of the Joint Information Governance Board will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

Keep lists in alphabetical order

ABBREVIATION	DEFINITION
AHRA	Access to Health Records Act 1990
CEO	Chief Executive Officer
CPFT	Cumbria Partnership NHS Foundation Trust
DPA	Data Protection Act 1998
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DS&Ptk	Data Security and Protection Toolkit
GDPR	General Data Protection Regulation
HSCIC	Health and Social Care Information Centre
ICO	Information Commissioner's Office
IAA	Information Asset Administrator
IAO	Information Asset Owner
IG	Information Governance
IGtk	Information Governance Toolkit
ISG	Information Sharing Gateway
MoU	Memorandum of Understanding
NCUH	North Cumbria University Hospitals NHS Trust
PID	Personal Identifiable Data
SAR	Subject Access Request
SIRO	Senior Information Risk Owner
SOP	Standard Operating Procedure
ToR	Terms of Reference

TERM USED	DEFINITION
Anonymised Information	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.
Confidentiality	A duty of confidence arises when one person discloses information to another person, where it is reasonable to expect that information is to be held in confidence.
Data Controller	A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. By person it does not necessarily mean a living individual but refers to legal entity (i.e. organisation).
Data Erasure	Also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Portability	The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the Data Controller.
Data Recipient	A recipient is any person who obtains a disclosure of data, this includes employees or agents who would not be regarded as third parties.
Data Subject	A natural person whose personal data is processed by a controller or processor
Disclosure	This is the divulging or provision of access to data.
Encrypted Data	Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access
Health Record	Information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual.
Healthcare Purposes	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
Information Asset Administrator	Primary role is to support the IAO to fulfill their responsibilities. IAAs will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information Asset Owners	Senior members of staff who take responsibility for Information Assets such as information systems - further defined in the Trust's Information Risk Policy.
Information Sharing Protocols	Documented rules and procedures for the disclosure and use of patient information, which specifically relates to security, confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001explicitly broadened the definition to include social care.
Personal Identifiable Information	Data that relate to a living individual who can be identified either from the data alone, or from combining the data with other information held by the data controller. It includes any recorded expression of opinion by or about the individual. Personal data may be held in electronic or manual form, or both.
Processing	Any activity that can be carried out concerning personal data.
Profiling	Any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

Pseudonymised Information	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
Sensitive Personal Data / Special categories of personal data	Under GDPR (article 9) "special categories of personal data" means personal data consisting of information such as: a) racial or ethnic origin b) political opinions, c) religious or philosophical beliefs d) trade union membership, e) genetic data f) biometric data g) health data h) sex life i) sexual orientation The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. The nature of the data is also a factor in deciding what security is appropriate
Third Party Information	Information relating to any person other than the data subject, the Data Controller or any data processor or other person authorised to process data for the controller or processor. Generally this would be one of the following: 1) Any individual who is identifiable from the records who is not the applicant. Note that this does not apply to healthcare professionals. 2) In an organisation context, a third party is any organisation / agency which is not the Trust, i.e. where the Trust holds information from other organisations, those other organisations remain organisationally responsible for their own records as the "data controller" and constitute third parties

DOCUMENT CONTROL

Equality Impact Assessment Date	Joint Data Protection Policy
Sub-Committee & Approval Date	*IG Performance Group – April 2018* *IG Board – May 2018.*

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published	Disposal Date
Data Protection Policy CPFT	1/5/17	31/5/18		28/6/18

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1 *(n=current version number)*	09/02/2018	• First draft written by Head of Information Governance • Circulated internally within team • Initial comments added •

n.2	09/03/2018	• Internal meeting with IG Team – comments added with flow chart
		  • Minor comments re numbering from Tony Atkinson
		  • Minor comment from Lorraine Gray

n.3		•

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Internal IG Staff (Anne Gadsden, Paul Corrie, Justine Gatehouse, Ruth Bunn)	Information Governance	9 February 2018 and 9 March 2018.
IG Performance Group	See full list of members in ToR	February 2018 April 2018
Human Resources Department IG Board members CCIO Sample of Information Asset Owners		16 March 2018.