King's College Hospital NHS
NHS Foundation Trust

Data Protection Policy

Main Document Information	
Version:	6.0
Publication Date:	
Approval Body (delete as appropriate)**:**	Information Governance Steering Group
Approval Date:	16/03/2017
Ratification Body (delete as appropriate)**:**	King's Executive / Board of Directors
Ratification Date:	
Document Author:	Data Protection office
Responsible Executive Director:	Chief Executive Officer
Review Date:	**31/01/2020**
Policy Category (delete as appropriate)**:**	Trust-wide
Document Change from Previous (delete as appropriate)**:**	Full Review following change to EU and UK Data Protection Legislation
Readership (Target Audience) (delete as appropriate)**:**	All Staff
Relevant External Requirements (CQC / NHSLA / HSE / DSPT etc.) **:**	DSPT / CQC / ICO

Document Location and History	
Current Document Title:	Data Protection Policy
Current Document Location:	http://King'sdoc/docs/policies
Current Document Replaces:	
Previous Document Name:	KCH Data Protection Policy DATAP 1998 & De-identification/Information handling for secondary use Policy v1.0
Previous Version Number:	4.01
Previous Publication Date:	03/2012
Location of Archived Document (delete as appropriate)**:**	http://King'sdocs/docs/policies/IT Policies

Document Authors		
Document Owner:	Data Protection Officer	
Other Contributing Authors:	Nicholas Murphy-O'Kane	
Consultation Distribution		
Sent To		**Date**
Group:	IGSG (by email)	
	Executive Management Team	
Team / Department:	ICT Security Team	08/02/2016
Data Subject:	Jo Downing	23/02/2017

Version Control History				
Version	**Date**	**Type of Change**	**Summary of Changes**	**Author**
5.0	15/03/2017	Full Review	Update of main policy and inclusion of appendices 3-10 and the previous De-identification policy	Jo Downing
5.1	1/6/2018	Full review following changes to Data Protection legislation	Major overhaul to reflect new legislation	Nicholas Murphy-O'Kane

Dissemination Schedule (Following Ratification)				
Target Audience	**Method of Distribution**	**Person Responsible**	**Confirmation Receipt Required?**	**Method of Replacement for Previous Version**
Trust Staff	Kingsdocs	Data Protection Officer	Yes	Replace previous version on Kingsdocs

Document Keywords	
Keywords:	Data; Data Protection; Data Protection policy; emailing patients; GDPR; sharing information; sharing patient information; sharing confidential information; email policy; scanning policy; faxing policy

Supporting Documentation (complete and added as appendices)	
Policy Checklist (delete as appropriate):	Yes
Equality Impact Assessment (delete as appropriate):	Yes
Ratification Sheet* (delete as appropriate):	Yes

* Ratification sheet stored centrally by the Policy Register Holder and not included as an appendix to this policy.

Contents

1: Introduction

King's College Hospital NHS Foundation Trust (KCH/Trust) needs to collect and process personal information about people with whom it deals or comes into contact with in order to carry out its business and provide its services in a safe and secure way. Such people will include users of our services (patients) visitors, employees (present, past and prospective), suppliers and other business contacts. Overall the personal information collected and processed includes (but is not limited to) name, address, telephone numbers, email address, data of birth, private and confidential information, special category information (also known as sensitive information) , criminal information and financial information. This information can be in a variety of formats including written (electronica nd manual, verbal or pictorial. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (DPA 18) and the EU General Data Protection Regulation 2016(GDPR) (the Acts).

The National Data Guardian and the Care Quality Commission (CQC) see the safety of patient data as a patient safety issue. All personal confidential data must be handled with care, and sensitive personal data must be handled with extra care. This policy is designed to enable staff to manage this information in line with statutory and regulatory requirements and protect both the Trust and Data Subjects from undue stress and concern and the risk of legal or disciplinary action as a result of breaches of confidentiality.

This policy sets out how the Trust will meet requirements concerning confidentiality, integrity and availability of the personal confidential information including the relevant and information security (physical and technical) which relate to personal-identifiable data. The requirements are based on the Acts (the key pieces of legislation covering the collection, use, security and confidentiality of personal information).

Furthermore, the Trust is committed to implementing the seven Caldicott principles for handling patient-identifiable information, namely:

1. Justify the purpose of using patient identifiable information.
2. Only use patient identifiable information when absolutely necessary.
3. Use the minimum necessary patient identifiable information.
4. Access patient identifiable information on a strict need to know basis.
5. Everyone should be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

2: Definitions

The following are definition / interpretations of phrases used within this policy and how they are to be used for this policy:

Term	Definition
Access to Health Records Act 1990	The act which was originally repealed by the DPA 1998 for living Data Subjects is still in place for information regarding deceased Data Subjects and their health information.
Caldicott Guardian	A named clinical lead that provides advice on the use of personal data (primarily patient focused) to the Trust Board and employees.
Commonly Used	This simply means that the format we choose must be widely-used and well-established. However, just because a format is 'commonly used' does not mean it is appropriate for data portability. We must consider whether it is 'structured', and 'machine-readable' as well. Although we may be using common software applications, which save data in commonly-used formats, these may not be sufficient to meet the requirements of data portability.
Consent	Consent is defined as: • Freely given; this means giving people genuine ongoing choice and control over how we use their data. • Obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly. • Specifically cover the Data Controller's name, the purposes of the processing and the types of processing activity. • Must be expressly confirmed in words, rather than by any other positive action. There is no set time limit for consent. How long it lasts will depend on the context. We should review and refresh consent as appropriate. Consent can also be removed at any time by the data subject.
Criminal Information	Information defined in the GDPR as personal data relating to criminal convictions and offences or related security measures.
Data	Data includes manual information held in structured files as well as information recorded in a form in which it can be processed automatically (i.e. by computer).
Data Agent	A Data Subject handling personal confidential data held by a Data Controller of Data Processor

Data Controller	A person or organisation who determines the purposes for and the manner in which personal data are, or are to be, processed. This may be a Data Subject, or an organisation and the processing may be carried out jointly or in common with other persons.
Data Masking	This involves stripping out obvious personal identifiers such as names from a piece of information, to create a data set in which no person identifiers are present. Variants: • Partial data removal – results in data where some personal identifiers, e.g. name and address have been removed but others such as dates of birth, remain. • Data quarantining - The technique of only supplying data to a recipient who is unlikely or unable to have access to the other data needed to facilitate re-identification. It can involve disclosing unique personal identifiers – e.g. reference numbers – but not the 'key' needed to link these to particular Data Subjects.
Data Processing	Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – (a) storage, organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.[1]
Data Processor	A person, who processes personal information on a Data Controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.
Data Protection Act 2018 (the Act)	The Data Protection Act (the Act) aims to give protection to all information relating to a living Data Subject. This includes information both processed by computers and held, stored manually in hard copy.
Data Protection Officer (DPO)	A Data Subject who is appointed by the Trust that co-ordinates all the Data Protection activities e.g. responsible for notification, training and monitoring of the Data Protection issues across the Trust. Liaises with all the systems

[1] Source : https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

	managers in respect of systems activity and Heads of Departments in respect of staff activity and training.
Data Subject	The Data Subject is the person or Data Subject who is the subject of the personal information (data). For the Trust this includes Staff, Patients Visitors and those that pass through our building s and surroundings.
Direct Care	The NHS Digital's Guide to Confidentiality defines *direct care* as: "A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of Data Subjects. It includes supporting Data Subjects' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the Data Subject has a legitimate relationship for their care."
EEA	European Economic Area.
EU General Data Protection Regulation 2016 (GDPR)	Regulation implemented by the EU Council in 2016
Freedom of Information Act (2000)	The Freedom of Information Act is law giving people the general right to see recorded information held by public authorities.
Health Data	This is data pertaining to the Physical and Mental Health of a Data Subject that is: • held by (or on behalf of) a Health Professional • not held by a Health Professional but was first recorded by or on behalf of a Health Professional.
Information Commissioner	The Information Commissioner is an independent official appointed by the Crown to oversee the Data Protection Act 2018, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.
Machine Readable	The Open Data Handbook states that 'machine readable' data is: 'Data in a data format that can be automatically read and processed by a computer.' Furthermore, Regulation 2 of the Re-use of Public Sector Information Regulations 2015 defines 'machine-readable format' as:

	'A file format structured so that software applications can easily identify, recognise and extract specific data, including Data Subject statements of fact, and their internal structure.' Machine-readable data can be made directly available to applications that request that data over the web. This is undertaken by means of an application programming interface ("API").
Notification	Notification is the process by which a Data Controller's processing details are added to a register. Under the Act every Data Controller who is processing personal data needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a Data Controller is exempt from notification, they must still comply with the principles.
Personal Identifiable Data/Information or Personal Confidential Data/Information (PII / PID / PCD)	Data which relates to a Data Subject who can be identified- from those data, or from those data and other information which is in the possession of, or likely to come into the possession of the Data Controller. It includes any expression of opinion about the Data Subject and any indication of the intentions of the Data Controller or any other person in respect of the Data Subject.
Processing	Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.
Profiling	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."
Secondary Use/Purpose	Information use not required for the direct care of the patient or primary process (e.g. employment or health system management). Examples include: performance monitoring, profiling, healthcare planning, commissioning, public health, governance, benchmarking, performance improvement, medical research and national policy development.
Senior Information Risk Owner (SIRO)	An Executive Director or Senior Management Board Member who has overall ownership of the Trust's Information Risk Policy, acts as champion for information risk on the Board of Directors.
Sensitive Personal Information	Sensitive personal data is information about a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trades' union membership, physical or mental health condition, sexual life, offences or alleged offences and information relating to any proceedings for

	offences committed or allegedly committed by the data subject, including the outcome of those proceedings.
Structured Data	‘data where the structural relation between elements is explicit in the way the data is stored on a computer disk.’ This means that software must be able to extract specific elements of the data. An example of a structured format is a spreadsheet, where the data is organised into rows and columns, i.e. it is ‘structured’. In practice, some of the personal data we process will already be in structured form. In many cases, if a format is structured it is also machine-readable.
Subject Access Request (SAR)	Under the Act Data Subjects can see the information about themselves that is held on computer and in most paper records. If a Data Subject wants more information on the personal data held about them, they can write to the person or organisation that they believe is processing the data.

3: Purpose and Scope

This policy covers personal-identifiable data in any format (including where the personal confidential data has been masked for further potential use) that relates to Data Subjects with whom the Trust has contact either directly or via an indirect method (e.g. CCTV). The Trust is registered as a Data Controller with the Information Commissioner under the Data Protection Act Regulations.

This policy also applies to all usage of Trust equipment that either stores or processes data in any way, Trust networks, databases, and access to the internet.

Users covered by this document are all employees and volunteers, plus any authorised third parties who may require access to the Trust’s email facilities or the Trust’s computers and networks: including contractors, sub-contractors, agents, temporary staff, those on work experience placements, students, and honorary staff.

The Trust’s contractors processing data (Data Processors) are required via contractual obligations to follow these standards and will be subject to audit by the Trust.

4: Roles and Responsibilities

4.1 Kings Executive Board of Directors

- Ensure that there is always a named lead (Data Subject person / named supplier) with overall responsibility for Data Protection.
- Ensure the Trust provides training for all staff members who handle personal information and,
- Provide clear lines of reporting and supervision for compliance with Data Protection requirements.
- Carry out regular checks to monitor and assess new processing of personal data and to ensure King's registration with the Information Commissioner is updated to take account of any changes in processing of personal data.
- Develop and maintain Data Protection procedures to include: roles and responsibilities, notification, subject access, training and compliance testing.

4.2 Information Governance Steering group (IGSG)

The IGSG have delegated accountability of the implementation and monitoring of this policy and its respective process documents (see Section 9).

The IGSG which is attended by the Senior Information Risk Owner, Caldicott Guardian and the Data Protection Officer will act as the named group to review Data Protection legislation and its implementation into business as usual in the Trust.

The IGSG will escalate specific key issues via its reporting to the Kings Executive Committee as well as the Audit Committee any key issues / risks that require escalation.

This group does not prevent the Data Protection Officer from requesting and attending the Trust Board, its formal committee and sub-committees as needed to provide support and advice for particular issues. But any such attendance will be noted at the IGSG.

4.3 Chief Executive

The Chief Executive has overall responsibility for compliance with Data Protection legislation within the Trust. As the executive lead, the Chief Executive will;

- Ensure that the Trust has appointed a suitable Data Protection Officer / Service (in accordance with the current criteria defined the Data Protection legislation) and
- Cascade this appointment to all Executive Managers, staff and 3rd parties as required.

4.4 Data Protection Officer (DPO)

The Trust is required under DP Legislation to appoint a Data Protection Officer. The role (which can be provided by a commissioned external provider), will report to the SIRO (Executive Director for Improvement, Information and ICT) but will be able to operate independently across the Trust as part of their duties.

The Data Protection Officer will:

- Provide information and advice to the company in relation to Data Protection issues including their obligations in relation to Data Protection
    - ensure compliance with all aspects of the Data Protection legislation and related provisions and provide reports to the senior level of management in the organisation;
    - draft and/or maintain the Trust Data Protection policy and procedures;
    - ensure service users are provided with information on their rights under Data Protection legislation;
    - devise and produce quarterly performance reports in relation to the implementation and compliance with Data Protection legislation
    - develop common actions and standards that can be applied across the local health community – in particular common information sharing agreements;

- Monitor compliance with Data Protection legislation completing relevant audits of services (including commercial obligations) and elements of the Data Security and Compliance toolkit.
    - promote Data Protection, Caldicott, Confidentiality and Information Security awareness throughout the organisation by organising training and providing written procedures that are widely disseminated and available to all staff;
    - co-ordinate the work of other staff with Data Protection responsibilities;
    - monitor compliance with the Acts and the effectiveness of procedures through the use of compliance checks / audits and ensure appropriate action is taken where non-compliance is identified;
    - complete annual external assessments for the Trust's performance against Confidentiality and Data Protection standards and produce organisation specific improvement plans;

- Provide advice where needed in regard to Data Protection by Design and Data Privacy Impact Assessments as needed.
    - keep up-to-date on developments in relation to Confidentiality and Data Protection on a local, patch wide and national level and advise on the implications for the Trust;
    - work with other agencies, for example Social Services and the Police to develop Information Sharing Agreements and ensure that the necessary policies and procedures are in place to underpin the agreements;
    - work with each service area to help develop and improve their specific action plans;
    - develop local networks for sharing best practice and exploiting opportunities to work collaboratively;
    - Oversee the Information Asset Register which is managed operationally by the IG manager, ensuring that Information Asset Owners complete relevant training;

- Act as central point of contact with the Information Commissioners Office, including consultation with them in relation to Overseas / Complex data processing, Incident reporting and management of incidents and other relevant consultations required.
    - maintain the Trust's registration with the Information Commissioner; ensuring accuracy and updating were appropriate;
    - assist with investigations into complaints about breaches of the Acts
    - act as a focal point on detailed Data Protection, Caldicott and Confidentiality queries within the Trust;

The Trust will ensure that this role is supported and resourced appropriately for the safe and effective delivery of its duties. The trust will also ensure that the contact details of the DPO will be published internally and externally via its web site.

4.5 Senior Information Risk Owner (SIRO)

Executive responsibility for compliance with this policy is delegated to the SIRO; and to all Information Asset Owners, in relation to the confidentiality of personal data within their assets.

The SIRO role will be in addition to other job responsibilities and to avoid confusion this extra role should be identified clearly within the SIRO's job description with appropriate weighting.

The SIRO's key responsibilities are:

- Leading and fostering a corporate culture that values, protects and uses information for the success of the organisation and benefit of its patients
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs.
- Advising the Chief Executive on the information risk aspects of their statement on internal controls.
- Owning the organisation's information incident management framework

The SIRO is supported in these responsibilities by the Deputy SIRO and this should similarly be identified in their job description with appropriate weighting.
The SIRO will:

- Chair the Information Governance Steering Group (IGSG).
- Represent confidentiality and security issues at Trust Board level.
- Oversee the development of an Information Risk Policy and a Strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues

4.6 Deputy SIRO

The Deputy SIRO will:

- Deputise for the SIRO as Chair of the IGSG.

- Deputise for/represent the SIRO as required in relation to information governance and Data Protection matters.
- Be responsible for Information Governance strategy, programme and structure and delivery of the Trust's requirements for compliance with the Data Security and Protection Toolkit (DSPT) and relevant statute including but not limited to the Acts and FOI Act. This will include close working with other key roles such as DPO to delivery against requirements.
- Monitor delivery of the strategy and provide reports to the IGSG and King's Executive and other bodies as required.

4.7 Caldicott Guardian

The Caldicott Guardian will:

- Act as the 'conscience' of the Trust regarding confidentiality and ensure that the Trust satisfies the highest practical standards for the handling of patient information, both within the Trust and data flows to other NHS and non-NHS organisations.
- Ensure that there is a framework enabling Caldicott principles to be reflected in Trust's policies and procedures for the management and use of personal information.
- Support the Information Governance team (Information Governance Manager, Data Protection Officer and Deputy SIRO) in the development of information sharing protocols.
- Offer support and advice as required to the Information Governance Team on matters relating to confidentiality and patient information.
- Sign off the Confidentiality and Data Protection components of the Information Governance Toolkit before submission to the IG Committee and the Board.
- Agree and review policies regarding the protection and use of personal information.
- Agree and review protocols governing the disclosure of personal information to partner organisations.
- Make the final decision in issues that arise regarding the protection and use of personal information, including where identifiable data is sent outside the Trust for secondary use purposes.

4.8 Information Asset Owners (IAOs) and Administrators (IAAs)

IAOs, supported by the relevant IAAs are responsible for:

- **Promoting** the culture that values, protects and uses their assigned information assets appropriately for the success of the organisation and benefit of its patients

- **Knowing** what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset

- **Knowing** who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with Trust policy. Understanding and addressing risks to the asset, and providing assurance on the management of information assets and their associated risks to the SIRO

It is important to distinguish IAOs from staff who have been delegated the responsibility for day to day management of information risk of an asset on behalf of the IAOs; the IAAs. The

IAAs are accountable to the IAOs. The SIRO/IAO hierarchy identifies accountability and authority to effect change where required to mitigate identified risk.

4.9 Line Managers

Line managers will ensure that staff check that any service user, student, staff or other Data Subject's information they handle is as accurate and as up–to-date as possible. They are also responsible for ensuring that all the staff they manage are up-to-date with their Information Governance training on an annual basis.

4.10 All staff

All employees, volunteers and students working at the Trust, who record and/or process personal data in any form must ensure that they comply with:

- the requirements of the Act (including the Data Protection principles)
- this policy, including any related procedures and guidelines which may be issued from time to time.
- the Subject Access Policy

Agencies, sub-contractors or any other organisation providing staff that may have access to or be involved in the processing of personal data held by the Trust will be required to complete a confidentiality agreement and be required to provide proof of compliance with the above standards within their own organisation.

The responsibilities of all staff are:

- Observe all forms of guidance, codes of practice and procedures about the collection, use and storage of personal information.
- Understand fully the purposes for which KCH uses personal information.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by KCH to meet its service needs or legal requirements.
- Ensure the information is correctly input into KCH systems.
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.
- On receipt of a request from a Data Subject for information held about them by or on behalf of immediately notify their line manager.
- Not send any personal information for secondary purposes outside the Trust without authorisation of the Caldicott Guardian.
- Not send any personal information outside of the United Kingdom without the authorisation of the Caldicott Guardian.
- Understand that breaches of this Policy may result in disciplinary action, including dismissal

5 Policy Specific Information

5.1 What is Personal Data

Personal data provided by or to the Trust must be processed in accordance with the Act. Data about a Data Subject will only be processed for lawful and fair purposes. The Trust

determines the manner and purposes for which personal data may be used. All purposes will be notified to the Information Commissioner as part of the Trust register.

For clarity, this includes employee data, patients and visitors.

5.1.1 Personal Data

Personal Data is information that relates to an identified or identifiable Data Subject. This can include deceased Data Subjects (NDG Guidance). This means that information that we have and can readily have access to can identify a Data Subject.

Under the new legislation, this format must be considered also when sharing data with other parties, and consideration if they have access to further information that can identify a Data Subject.

Examples of personal identifiable data include (but not limited to) name, identification number, bank details, location data, online identifier (e.g. IP address or cookies), Car Registration Number or digital images (pictures) of a face

Processing of personal data requires a legal basis as set out in Article 6 of the EU GDPR Regulations.

5.1.2 Sensitive Personal Data

In additional to personal data, the Data Protection legislation defined certain data types as special category data or Sensitive personal data. This is because this data is more sensitive and so needs more protection.

These data groups include race, ethnic origin, political views; religion; trade union membership; genetics; biometrics (where used for ID Purposes); health data; sexual activity and orientation and educational data.

Processing of these data types requires a GDPR Article 9 legal basis. This does not have to be the same as that used in Article 6 (Personal Data) but the most suitable to the purpose for the processing.

5.1.3 Criminal Data

Criminal data is that information relating to a Data Subject's criminal convictions or offences, including allegations, proceedings or convictions. To process this data group, in addition to the Article 6 (Personal Data) requirement, the Trust must have a legal authority or official authority to do so. This is identified as Compliance with Article 10.

In line with the Trust departments / processing activity, the following are the key areas where such processing is approved:

- Workforce (Disclosure and Barring for relevant employees)
- Counter Fraud (Fraud and Bribery Investigation)
- Security (Criminal allegations)
- Safeguarding (Allegations / proceedings / convictions)
- Havens / Sexual Health (Allegations / proceedings / convictions)

Where additional processes are requested to use criminal data, these must be approved by the Trust DPO and SIRO.

5.2 Controllers and Processors

The Trust operates in a variety of different roles and responsibilities in regard to Data Protection Legislation. This means that when considering Data Protection and the impacts / roles and responsibilities we need to be able to identify which function we (*the Trust) are operating in. The following outline the relevant categories:

5.2.1 Data Controller

A Data Controller is the key person or organisation that determines the use of personal data. They exercise the control over the purpose and means of processing.

As Data Controller the Trust will be the lead organisation ensuring compliance with the Data Protection legislation both for itself and any other third party in contracts to support the processing of personal data.

5.2.2 Joint Data Controller

A joint Data Controller (also commonly described as Data Controller in common) will work together to determine the use and purpose of personal data

5.2.3 Data Processor

A Data Processor ONLY acts on the instruction of the Data Controller (including Joint Data Controllers). A Data Processor MUST be registered to process personal data with the Information Commissioner's Office

5.3 Data Protection Principles

There are six key principles within the Act, normally referred to as the 'Data Protection principles.

Accountability Principles requires the Trust and each member of staff to take responsibility for what they do with personal data and how they comply with the other Data Protection principles.

The Trust will have appropriate measures and records in place to be able to demonstrate its compliance.

There are a number of measures that we can, and in some cases must, take including:

- adopting and implementing Data Protection policies;
- taking a 'Data Protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out Data Protection impact assessments for uses of personal data that are likely to result in high risk to Data Subjects' interests;
- appointing a Data Protection Officer; and

- adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing and must be reviewed and, where necessary, updated.

5.3.1 Principle 1 – Lawfulness, Fairness and transparency

Personal data shall be processed fairly and lawfully.

This means that we must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the Data Subjects concerned;
- be transparent about how we intend to use the data, and give Data Subjects appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways that they would reasonably expect; and
- make sure we do not do anything unlawful with the data.

The Trust achieves this through its Privacy Notification published on its web site. The Data Protection Officer and IGSG will review the notification on a regular basis to ensure it remains relevant to activities completed by the Trust.

In addition to our main Privacy Notice for general activity, the Trust will maintain two additional notices covering use of staff data and research.

5.3.2 Principle 2 – Purpose Limitation

Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

The purposes for which personal information about living Data Subjects is obtained, held, and/or processed on any Trust systems, must be registered with the Office of the Information Commissioner. It is the responsibility of the Data Protection Officer to submit an appropriate notification for the Trust on an annual basis and to ensure the notification is accurate. The notification must be updated with any relevant changes to hardware, software or process.

Data held on Trust systems must only be used for the purpose for which it was collected, and any additional use can only be authorised with the specific permission/consent of the data subject(s) concerned.

For help with assessing the risks associated with handling data contact the Trust DPO.

5.3.3 Principle 3 – Data Minimisation

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Commonly known as the adequacy principle, it obliges the Trust, as Data Controller, to obtain only the minimum information that is necessary for the purpose, or purposes, of processing the data.

Consideration of the format of data should also be included here with and the lowest level of data ONLY used, these formats are;

- **Clear Data** (fully identifiable information).

- **Pseudonymised** - where key data are converted to a pseudo code) This process MUST be in line with the ICO Code of Practice. Pseudonymised data is still classed as personal data and must be managed similar to clear data, including identifying where other data may be linked (and if this could identify the Data Subject). This data format can be re-identified.

- **Anonymised** – where data is truly de-identified so that it cannot be re-identified.

- **Aggregate** – where the data is in groups only and cannot be identified down to a Data Subject.

    - Less than 5 records can be considered as too few to provide adequate minimisation and where aggregate figures fall below this level other formats must be considered and used.

Staff should consider the minimum level of information required and the format that these could be provided in.

Further information is available in the Data Minimisation procedures available on Kwiki.

5.3.4 Principle 4 - Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Accuracy of information can be achieved by implementing validation routines; some of which will be system specific and details will be provided of these validation processes to the system/information users. Staff who are responsible for inputting data into the Trust systems are responsible for the:

- quality
- accuracy
- timeliness
- completeness of the data.

Staff have a duty to check with patients that the information held by the Trust is up to date by asking patients attending appointments to validate the information held. Data Subject staff have a duty to inform Workforce Development (Workforce) of any changes in their personal data. Workforce should also actively check staff information for accuracy on a regular basis.

5.3.5 Principle 5 – Storage Limitation (previously known as the Retention Principle)

Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

All records subject to the Act should be kept in line with the Trust Records Retention Schedule (based upon the NHS Records Management Code of Practice 2016 document produced by the Information Governance Alliance).

Where any records are required to be retained beyond the minimum standards, a formal request must be made to the IGSG for approval. The IG manager / DPO will retain a formal log of all requests and decisions.

5.3.6 Principle 6 - Integrity and Confidentiality (Security)

The Trust must ensure that we have appropriate security measures in place to protect the personal data we hold. This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

To ensure the safety and integrity of all personal data the Trust must look to take steps to put in place technical solutions to protect data. These are covered in the KCH ICT Information Technology Security Policy.

For note, organisational solutions include;

- Organisations security measures
  - e.g. Clear Desk standards and automatic screen timeouts
- ICT and CEF Security Policies
- Workforce procedures
  - e.g. DBS checks
- Risk Management
- Training and Awareness

All staff (or students, volunteers etc.) with access to Trust systems, in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that neither the Trust, nor any Data Subject employed by the Trust, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All Data Subjects must fully comply with this and other related Trust policies and procedures.

When data is processed by a 3rd party Data Processor on behalf of the Trust, the Trust must ensure a contract is in place and, that under this contract, the Data Processor is only to act under instructions of the Trust. The contract must also require the 'Data Processor' to comply with obligations equivalent to those imposed on the Data Controller by the 7th Principle.

The Trust will take all reasonable steps to ensure that the Data Processor is complying with Principle 7 and that they give appropriate guarantees against non-compliance, i.e. indemnity for any of the Principles breached within the Act.

5.4 Lawful Basis for Processing

Personal data shall be processed in accordance with the rights of data subjects under this Act. This is broken down into 3 key categories for legal basis

- Article 6 - Personal Data
- Article 9 - Sensitive Personal Data
- Article 10 - Criminal Data

When considering the processing of personal data, the Trust supported by the DPO will define which area for each category is appropriate (there can be more than one legal basis in the first two articles

In all cases, the legal basis **MUST** be identified and recorded prior to the collection of any new data or change in the purpose is approved.

There are a number of identified legal basis for processing personal data which are outlined below;

5.4.1 Article 6 – Legal Basis for Processing Personal Data

In accordance with the new legislation for each processing activity of personal data, the Data Controller must ensure that it has a legal basis for the processing. To achieve this for each processing of personal data must be aligned to at least one of the following;

a) **Consent:** The Data Subject has given clear consent for the Trust to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract the Trust have with the Data Subject, or because they have asked us to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for the Trust to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for the Trust to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for the Trust legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the Data Subject's personal data which overrides those legitimate interests. (This cannot apply if we are a public authority processing data to perform our official tasks.)

5.4.2 Article 9 – Legal Basis for Processing Sensitive Personal Data

If the processing then relates to sensitive personal data, the Trust will then need to identify at least one of the following:

a) **Explicit Consent** - the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
b) **Obligations o/ Specific Rights** - 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.
c) **Vital Interests** - 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) **Legitimate Activities** - 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) **Already Made Public** - processing relates to personal data which are manifestly made public by the data subject;
f) **Legal Claims** - processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
g) **Public Interest** - processing is necessary for reasons of substantial public interest,

h) **Preventative or Occupational Medicine** - 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.
i) **Public Health** - 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,
j) **Research** - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5.4.3 Article 10 – Legal Basis for Processing Criminal Data

To process personal data about criminal convictions or offences, we must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.

The Trust can also process this type of data if we have official authority to do so because we are processing the data in an official capacity.

5.4.4 Consent

Regarding the most common data processing applications used in the Trust such as **Direct Patient Care** including system management (management of our patients), **Employment** (management of our staff) and **Crime Prevention** (e.g. counter fraud, CCTV and general physical security) the Trust rely on various legal basis identified in the DPA 2018 to use this. Where this takes place, the Trust will ensure clear, transparent notification is provided via its Privacy Notice.

However, for any other use of personal data, commonly described as secondary purposes, the Trust seeks and obtains “explicit consent” whenever practicable from the Data Subject or their representative.

This approach is to allow Data Subjects an opportunity to raise any objections to any intended processing of their personal data.

The Trust will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by UK Data Protection and are identified in our Privacy Notice.

The criteria for valid consent are

- Consent must be freely given; this means giving people genuine ongoing choice and control over how we use their data.
- Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
- Consent must specifically cover the Data Controller’s name, the purposes of the processing and the types of processing activity.
- Explicit consent must be expressly confirmed in words, rather than by any other positive action.

When consent is collected, the relevant Information Asset Owner must ensure that a process is in place to also receive changes of consent and ensure that these can be actioned.

The DPO will provide advice on best practice and also report on activity to the IGSG.

5.5 Data Subject Rights

The Act sets out a number of rights for Data subjects; below is a summary list of Data Subjects' rights which are relevant to the Trust:

5.5.1 General Statements regarding the rights and their application

5.5.1.1 Making a request about their rights

New Data Protection legislation does not specify how to make a valid request. Therefore, a Data Subject can make a subject access request to the Trust verbally or in writing (including email). It can also be made to any part of our organisation (including by social media) and does not have to be to a specific person or contact point.

A request does not have to include the specific phrases of the rights they wish to invoke, if it is clear that the Data Subject is asking for a specific task.

To support staff, where a verbal request is made, the staff member should direct the applicant to the PALS services (if made while on a Trust site) or through to our Internet site to make application.

All requests will be recorded in line with the Trust policy.

5.5.1.2 Fees

In most cases the Trust cannot charge a fee to comply with a request related to the Data Subject's rights and their application. However, if the request is manifestly unfounded or excessive, we may charge a "reasonable fee" for the administrative costs of complying with the request.

5.5.1.3 Timeframe

The Trust must act upon the request without undue delay and at the latest within one month of receipt based on the time limit from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the Data Subject. If extensions are required, we must inform the Data Subject without undue delay and within one month of receiving their request and explain why the extension is necessary. Any extensions will be reported via the IGSG.

The circumstances in which we can extend the time to respond can include further consideration of the accuracy of disputed data - although we can only do this in complex cases - and the result may be that at the end of the extended time period we inform the Data Subject that we consider the data in question to be accurate.

However, based on advice from the ICO's the Trust consider that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- we are requesting proof of identity before considering the request.

5.5.1.4 Proof of ID

Where a request is made and we have doubts about the identity of the person making the request, the Trust we can ask for additional information. However, it is important that we only request information that is necessary for identification purposes (e.g. passport / driving licence).

In these circumstances, we will advise the applicant without undue delay and within one month that additional information is required from them to confirm their identity.

Where additional requests are made, the timeline for the relevant request is suspended.

5.5.2 Right to be Informed

5.5.2.1 General Overview

Data Subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the Data Protection legislation. The Trust provide this via various Privacy Notifications including the main Privacy Notice published on our Internet.

In addition to this approach, local departments / projects will use more general notices about processing of data including posters, information leaflets and verbal discussion which are acceptable.

All notifications must include the following key information and be provide **before** any processing occurs

- The purposes for processing their personal data,
- Our retention periods for that personal data,
- Who it will be shared with (including all secondary sharing)?

Where privacy notices relate to data processed about children, the Trust will take additional steps to ensure that the notices provide are appropriately written, using clear and plain language.

For all audiences, we must provide information to them in a way that is in line with the Accessible Information Standards and is:

- **concise;**
- **transparent;**
- **intelligible;**
- **easily accessible; and**
- **uses clear and plain language**

Privacy notices can be provided by of one the following techniques:

- **A layered approach** – typically, short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how we use their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time we collect Data Subject pieces of information about people.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

When we are considering new processes the context in which we are collecting personal data and its audience will be included in the decision.

5.5.2.2 Exceptions

There are a few circumstances when we do not need to provide users / visitors with privacy information, such as if a Data Subject already has the information or if it would involve a disproportionate effort to provide it to them.

5.5.3 Right of Access

5.5.3.1 General Overview

In accordance with the legislation any Data Subject has the right to access what personal information is being processed by the Data Controller. The Trust manages this rule under the Trust Subject Access Policy

Access to records may also be covered under the Freedom of Information Act and all procedures relating to disclosure of information must consider both the Act and Freedom of Information Act 2000. The Access to Health Records Act 1990 deals with access to records of people who have died.

Data Subjects have the right to obtain the following from us:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that we should provide in a Privacy Notice (see 'Other information' below).

In addition to a copy of their personal data, we also have to provide Data Subjects with the following information:

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;
- our retention period for storing the personal data or, where this is not possible, our criteria for determining how long we will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;

- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the Data Subject;
- the existence of automated decision-making (including profiling); and
- the safeguards we provide if we transfer personal data to a third country or international organisation.

We may be providing much of this information already in our Privacy Notice.

Further details of the Subject Access process can be found in the Trust Subject Access Policy.

5.5.4 Right to Rectification

5.5.4.1 General Overview

A Data Subject has the right to have inaccurate personal data rectified by the Data Controller. Applicants may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data by the relevant professions (clinical or administrative).

This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). However, although we may have taken steps already to ensure that the personal data was accurate when we obtained it; this right imposes a specific obligation to reconsider the accuracy upon request.

Upon a request for rectification, the relevant Lead Manager supported by the DPO and SIRO will take reasonable steps to reasonable action to ensure that the data in question is accurate and to rectify the data if necessary.

For generic terms, the level of accuracy is based on the Data Protection Act 2018 (DPA 2018) which states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In these circumstances the fact that a mistake was made, and the correct information should also be included in the Data Subject's data.

When investigating a query on accuracy, the Trust will try to restrict access / processing of the data while issues are being resolved. In most cases, this will be completed by the inclusion of a note on the Data Subject record outlining the challenge.

Where a request for rectification is made, and accepted, the Trust is responsible to notify any 3rd party of the change. For key systems (e.g. the SEL Local Care Record) it will be essential to notify all parties vita the LCR operational team.

5.5.4.2 Exceptions

Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information

is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

5.5.4.3 Refusing a Request

If the Trust decides that the information in question is accurate, a formal record of the review will be placed on the Data Subjects record and the Data Protection Officer will inform the applicant of the decision and the justification behind this. Refusal of the request, does not prevent the applicant contacting the ICO

5.5.5 Right to Erasure

5.5.5.1 General Overview

The new DP legislation allows for the right to have information erased also known as the right to be forgotten. This is applied only in specific circumstances if;

- the personal data is no longer necessary for the purpose which it was originally collected or processed ;
- we are relying on consent as the lawful basis for holding the data, and the Data Subject withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the Data Subject objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the Data Subject objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

Where the Trust agrees to erase personal data, we will need to ensure the following

- Ensure that all relevant 3rd parties (e.g. LCR) are notified of the request and the erasure and the action taken
- Backups will need to be considered and where possible included in the erasure process, these can be fulfilled by;
    - Consideration of normal lifecycle
    - Cost implications of forced deletion for backup(s)

5.5.5.2 Special Impact on Children

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the current legislation.

Therefore, where the Trust processes data collected from children, we will give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the Data Subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

5.5.5.3 Exceptions

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.
- if the processing is necessary for public health purposes in the public interest (e.g. 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); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services).
    - This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

These exemptions mean that ALL clinical records are NOT subject to erasure, but the right of Restriction MUST then be considered by the Trust.

5.5.6 Right to Restrict Processing

5.5.6.1 General Overview

The right to restrict the processing of their personal data in certain circumstances. This means that a Data Subject can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Data Subjects have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information held or how we have processed their data.

In most cases we will not be required to restrict a Data Subject's personal data indefinitely but will need to have the restriction in place for a certain period of time.

Data Subjects can request restriction for the following reasons:

- the Data Subject contests the accuracy of their personal data and we are verifying the accuracy of the data (See right to rectification);
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle) and the Data Subject opposes erasure and requests restriction instead;
- we no longer need the personal data, but the Data Subject needs us to keep it in order to establish, exercise or defend a legal claim; or

- the Data Subject has objected to us processing their data, and we are considering whether our legitimate grounds override those of the Data Subject.

Depending on the nature of the data, Trust and local managers and employees will adopt one of the following activities where possible:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website (where applicable).

However, the policy and the Trust Board recognise that for our main computer systems restriction in many of these systems is not technically possible. In these cases, the DPO will create a list of persons that have requested restriction and periodically seek assurance that these records have not been accessed.

This process will be cascaded to the Data Subject at the time of the request.

Once data is restricted, the Trust and its employees recognise that we cannot carry out any further processing unless

- we have the Data Subject's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the Data Subject has disputed the accuracy of the personal data and we are investigating this; or
- the Data Subject has objected to us processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of our legitimate interests, and we are considering whether our legitimate grounds override those of the Data Subject.

Once the Trust has decided on the accuracy of the data, or whether our legitimate grounds override those of the Data Subject, we may decide to lift the restriction following consultation with the Data Subject.

5.5.7 Right to Data Portability

5.5.7.1 General Overview

The right to data portability gives Data Subjects the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

The right to data portability only applies when:

- the trust lawful basis for processing this information is consent or for the performance of a contract (Article 6 a and b) and (Article 9(a and b); and
- we are carrying out the processing by automated means (i.e. excluding paper files).

Information is only within the scope of the right to data portability if it is personal data of the Data Subject that they have provided to us.

The meaning of data 'provided to' the Trust by the Data Subject will also include personal data resulting from observation of a Data Subject's activities (e.g. where using a device or service).

This may include:

- history of website usage or search activities;
- traffic and location data; or
- 'raw' data processed by connected objects such as smart meters and wearable devices.

It does not include any additional data that we have created based on the data a Data Subject has provided to us. For example, if we use the data, they have provided to create a user profile then this data would not be in scope of data portability.

The right to data portability only applies to personal data. This means that it does not apply to genuinely anonymous data. However, pseudonymous data that can be clearly linked back to a Data Subject (e.g. where that Data Subject provides the respective identifier) is within scope of the right.

If the requested data has been provided to, us by multiple persons / another organisation (e.g. change of commissioned service) the Trust need to be satisfied that all parties agree to the portability request. This means that we (or the commissioner) may have to seek agreement from all the parties involved.

The right to data portability entitles a Data Subject to:

- receive a copy of their personal data; and/or
- have their personal data transmitted from one controller to another controller.
- Data Subjects have the right to receive their personal data and store it for further personal use. This allows the Data Subject to manage and reuse their personal data. For example, a Data Subject wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store.

This right does not create an obligation for the Trust to allow Data Subjects more general and routine access to our systems – only for the extraction of their data following a portability request.

In relation to the transfer of the data, where Data Subjects have the right to ask us to transmit their personal data directly to another controller without hindrance. If it is technically feasible, we should do this.

The Trust will consider the technical feasibility of each transmission on a request by request basis. The right to data portability does not create an obligation for the Trust to adopt or maintain processing systems which are technically compatible with those of other

organisations. However, we will take a reasonable approach, and this should not generally create a barrier to transmission.

Where the Trust provide information directly to a Data Subject or to another organisation in response to a data portability request, we are not responsible for any subsequent processing carried out by the Data Subject or the other organisation.

However, we are responsible for the transmission of the data and need to take appropriate measures to ensure that it is transmitted securely and to the right destination and will advise applicants of the security implications of such a transfer.

The Trust will make every effort to provide the personal data in a format that is:

- structured;
- commonly used; and
- machine-readable.
- an interoperable format (where applicable suitable to Trust systems)

When the Trust receives personal data that has been transmitted as part of a data portability request, we will action the request in line with local policy and procedure (including this policy).

5.5.8 Right to Object

5.5.8.1 General Overview

Data Subjects have the right to object to the processing of their personal data. This effectively allows Data Subjects to ask us to stop processing their personal data. The right to object only applies in certain circumstances, and whether it applies depends on the Trust purposes for processing and its lawful basis for processing.

Data Subjects have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Data Subjects can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in us; or
- Our legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute. Where the Trust is processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

Where an objection to process is received the Trust must inform the Data Subject without undue delay and within one month of receipt of the request.

We will tell the Data Subject about:

- the reasons we are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

In addition to this right, the National Data Guardian and NHS Digital have introduced a "National Opt out" capability aligned to secondary use of NHS patient data. The Trust will follow all guidance issued by the National Data Guardian's office and make every reasonable effort to ensure that these decisions recorded on the NHS Care Records Service are fully respected.

5.5.9 Rights related to automated decision-making including profiling

5.5.9.1 General Overview

Profiling is now specifically defined in the GDPR. Solely automated Data Subject decision-making, including profiling with legal or similarly significant effects is restricted.

There are three grounds for this type of processing that lift the restriction. Where one of these grounds applies, we must introduce additional safeguards to protect Data Subjects. These work in a similar way to existing rights under the 1998 Data Protection Act.

Data Protection legislation requires the Trust to provide the Data Subjects with specific information about automated Data Subject decision-making, including profiling.

The Trust can carry out solely automated decision-making with legal or similarly significant effects only if the decision is:

- necessary for entering into or performance of a contract between an organisation and the Data Subject;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the Data Subject's explicit consent.

If we're using special category personal data, we can carry out processing described only if:

- we have the Data Subject's explicit consent; or
- the processing is necessary for reasons of substantial public interest.

Because this type of processing is considered to be high-risk the Data Protection legislation requires us to carry out a Data Protection Impact Assessment (DPIA) to show that we have identified and assessed what those risks are and how we will address them.

As well as restricting the circumstances in which we can carry out solely automated Data Subject decision-making the Data Protection Legislation also:

- requires us to give Data Subjects specific information about the processing;
- obliges us to take steps to prevent errors, bias and discrimination; and
- gives Data Subjects rights to challenge and request a review of the decision.

These provisions are designed to increase Data Subjects' understanding of how we might be using their personal data.

Where we carry out this function, the Trust will provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the Data Subject;

- use appropriate mathematical or statistical procedures;
- ensure that Data Subjects can:
    - obtain human intervention;
    - express their point of view; and
    - obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that we can correct inaccuracies and minimise the risk of errors;
- secure personal data in a way that is proportionate to the risk to the interests and rights of the Data Subject, and that prevents discriminatory effects.

5.6 Accountability and Governance

5.6.1 Contracts / Commercial

The Data Protection legislation makes written contracts between controllers and processors a requirement, rather than just a way of demonstrating compliance with the sixth Data Protection principle (appropriate security measures) under the Data Protection Act 2018.

These contracts must now include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the GDPR requirements, not just those related to keeping personal data secure.

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties.

Similarly, if a processor uses another organisation (i.e. a sub-processor) to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor.

Contracts between controllers and processors ensure they both understand their obligations, responsibilities and liabilities. Contracts also help them comply with the GDPR and assist controllers in demonstrating to Data Subjects and regulators their compliance as required by the accountability principle.

What needs to be included in the contract?

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of Data Subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- Data Subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

Data Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet GDPR requirements and protect Data Subjects' rights.

Controllers are primarily responsible for overall compliance with the GDPR, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the GDPR. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to the Data Protection Legislation must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

5.6.2 Data Protection by Design and Default

The Data Protection legislation introduces new obligations that require the Trust to integrate Data Protection concerns into every aspect of our processing activities. This approach is 'Data Protection by design and by default'. These are key elements of the GDPR's risk-based approach and its focus on accountability, i.e. we can demonstrate how we are complying with its requirements.

However, Data Protection by design and by default is not new. It is essentially the Data Protection legislation's version of 'privacy by design', an approach that the Trust has championed for many years. Although privacy by design and Data Protection by design are not precisely the same, there are well-established privacy by design principles and practices that can apply in this context.

Data Protection by design is ultimately an approach that ensures we consider privacy and Data Protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the Data Protection legislation, it requires us to:

- put in place appropriate technical and organisational measures designed to implement the Data Protection principles; and
- integrate safeguards into our processing so that we meet the GDPR's requirements and protect the Data Subject rights.
- This means we have to integrate or 'bake in' Data Protection into our processing activities and business practices.
- Data Protection by design has broad application. Examples include:
- developing new IT systems, services, products and processes that involve processing personal data;
- developing organisational policies, processes, business practices and/or strategies that have privacy implications;
- physical design;

- embarking on data sharing initiatives; or
- using personal data for new purposes.

Data Protection by default requires us to ensure that we only process the data that is necessary to achieve our specific purpose. It links to the fundamental Data Protection principles of data minimisation and purpose limitation.

The Trust has to process some personal data to achieve our purpose(s). Data Protection by default means we need to specify this data before the processing starts, appropriately inform Data Subjects and only process the data we need for our purpose. It does not require us to adopt a 'default to off' solution. What we need to do depends on the circumstances of our processing and the risks posed to Data Subjects.

Nevertheless, we must consider things like:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring we do not provide an illusory choice to Data Subjects relating to the data we will process;
- not processing additional data unless the Data Subject decides we can;
- ensuring that personal data is not automatically made publicly available to others unless the Data Subject decides to make it so;
- providing Data Subjects with sufficient controls and options to exercise their rights; and
- Identification of who is responsible for complying with Data Protection by design and by default

If the Trust are using another organisation to process personal data on our behalf, then that organisation is a Data Processor under the Data Protection legislation.

In this regards Data Protection by design and by default can also impact organisations other than controllers and processors. Depending on our processing activity, other parties may be involved, even if this is just where we purchase a product or service that we then use in our processing. Examples include manufacturers, product developers, application developers and service providers.

Therefore, when considering what products and services we need for our processing, we should look to choose those where the designers and developers have taken Data Protection into account. This can help to ensure that our processing adheres to the Data Protection by design requirements.

Where we are a developer or designer of products, services and applications, the Data Protection legislation places no specific obligations on us about how we design and build these products. (We may have specific obligations as a controller in our own right, e.g. for any employee data.) However, we should note that controllers are required to consider Data Protection by design when selecting services and products for use in their data processing activities – therefore if we design these products with Data Protection in mind, we may be in a better position.

The Trust will put in place appropriate technical and organisational measures designed to implement the Data Protection principles and safeguard Data Subject rights which are

monitored by the IGSG. There is no 'one size fits all' method to do this, and no one set of measures that we should put in place. It depends on each set of circumstances.

Data Protection by design must be included at the initial phase of any system, service, product, or process. To achieve the best results, we must start by considering our intended processing activities, the risks that these may pose to Data Subjects, and the possible measures available to ensure that we comply with the Data Protection principles and protect Data Subject rights. These considerations must cover:

- the state of the available technical solutions and costs of implementation of any measures;
- the nature, scope, context and purposes of our processing; and
- the risks that our processing poses to the rights and freedoms of Data Subjects.

This is similar to the information risk assessment we do when considering our security measures.

The key is to take an organisational approach that achieves certain outcomes, such as ensuring that:

- we consider Data Protection issues as part of the design and implementation of systems, services, products and business practices;
- we make Data Protection an essential component of the core functionality of our processing systems and services;
- we only process the personal data that we need in relation to our purposes(s), and that we only use the data for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice, so that Data Subjects should not have to take any specific action to protect their privacy;
- the identity and contact information of those responsible for Data Protection are available both within our organisation and to Data Subjects;
- we adopt a 'plain language' policy for any public documents so that Data Subjects easily understand what we are doing with their personal data;
- we provide Data Subjects with tools so they can determine how we are using their personal data, and whether we are properly enforcing our policies; and
- we offer offering strong privacy defaults, user-friendly options and controls, and respect user preferences.

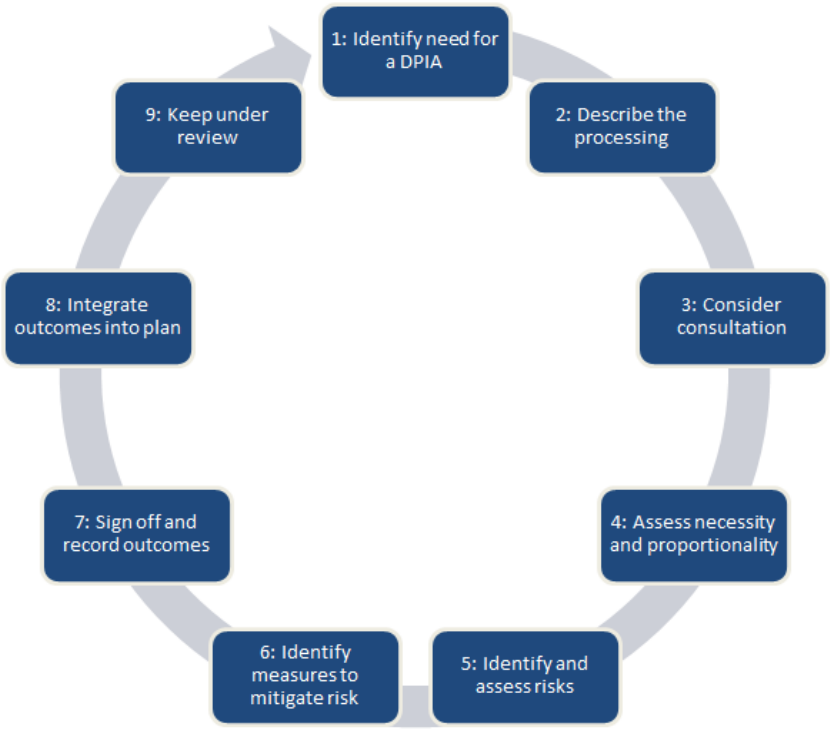
Many of these relate to other obligations in the Data Protection legislation, such as transparency requirements, documentation, Data Protection Officers and DPIAs. This shows the broad nature of Data Protection by design and how it applies to all aspects of our processing. Our guidance on these topics will help we when we consider the measures, we need to put in place for Data Protection by design and by default.

5.6.3 Data Protection Impact Assessment (DPIA)

The Trust has been introducing the DPIA format for the last few years. The new Data Protection Legislation moves this approach to a legal basis. All process, contracts, procedures and data usage planned MUST have an updated DPIA in place.

Any change in the processing activity will automatically require a full review of the previous DPIA.

The diagram below demonstrates the DPIA process adopted by the Trust



5.6.4 Certification

Certification is a way of demonstrating that our processing of personal data complies with the Data Protection legislation requirements, in line with the accountability principle. It could help us demonstrate to the ICO that we have a systematic and comprehensive approach to compliance.

Certification can also help demonstrate Data Protection in a practical way to other NHS services, Data Subjects and regulators.

The Data Protection legislation says that certification is also a means to:

- demonstrate compliance with the provisions on Data Protection by design and by default
- demonstrate that we have appropriate technical and organisational measures to ensure data; and
- to support transfers of personal data to third countries or international organisations

Applying for certification is voluntary. However, if there is an approved certification scheme that covers our processing activity, we may wish to consider working towards it as a way of demonstrating that we comply with the Data Protection legislation.

5.6.5 Data Protection Fee

On 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 (the 2018 Regulations) came into force, changing the way we fund our Data Protection work. Under the 2018 Regulations, organisations that determine the purpose for which personal data is processed (controllers) must pay a Data Protection fee unless they are exempt. The

new Data Protection fee replaces the requirement to 'notify' (or register), which was in the Data Protection Act 1998 (the 1998 Act).

The Trust is Tier 3 and pays the highest amount possible. Failure to pay on time/ensure that the registration is renewed correctly may lead to a fine.

The Trust will ensure that each year it reviews its Data Protection Compliance against registered activities and processes and renew or registration.

5.6.6 Complaints

The Trust will ensure that the complaints procedure is reviewed to take account of complaints which may be received because of a breach, or suspected breach, of the Act.

5.7 Data Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

To ensure the safety and integrity of all data, the Trust must look to take steps to put in place technical solutions to protect data, see the Information Technology Security Procedure for details.

Organisational solutions include:

- organisational security measures
- clear desk standards
- automatic screen timeouts
- security policies
- Workforce procedures – vetting etc.
- awareness and training programmes
- risk management
- pseudonymisation (see appendix 5)
- fax (appendix 6)
- post (appendix 7)
- emails and SMS (appendix 8)

.

All staff (or students, volunteers etc.) with access to Trust systems, in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that neither the Trust, nor any Data Subject employed by the Trust, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All Data Subjects must comply fully with this and other related Trust policies and procedures.

When data is processed by a 3rd party Data Processor on behalf of the Trust, the Trust must ensure a contract is in place and, that under this contract, the Data Processor is to act only under instructions of the Trust. The contract must also require the 'Data Processor' to comply with obligations equivalent to those imposed on the Data Controller by the 6th Principle.

The Trust will take all reasonable steps to ensure that the Data Processor is complying with Principle 6 and that they give appropriate guarantees against non-compliance, i.e. indemnity for any of the Principles breached within the Act.

All staff (including volunteers and contractors) and students within the Trust are responsible for ensuring that:

- any personal data which they hold is kept securely
- personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that all reasonable efforts will be made to ensure data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct, for guidance; please consult the Information Governance Manager or Data Protection Officer.

Personal data must be kept securely and examples of how this may be done will include:

- keeping data locked in a filing cabinet, drawer or room; or
- if the data is held digitally, ensuring that the data is password protected
- encryption

Further details of Data Security can be found in the trust ICT Information Security Policy, as well as local data security statements in Data Subject System Specific Information Security Policies (SSISP).

5.8 Personal Data Breaches

A 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then we must notify the ICO in line with the Trust Incident Management Policy; if it is unlikely then the Trust does not have to report it.

In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for Data Subjects. Which are:

- "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy

or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on Data Subjects, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect Data Subjects whose personal data has been compromised. We need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, we must try to contain it and assess the potential adverse consequences for Data Subjects, based on how serious or substantial these are, and how likely they are to happen.

If our organisation uses a Data Processor, and this processor suffers a breach, then under our contractual obligations it must inform us without undue delay as soon as it becomes aware.

This requirement allows us to take steps to address the breach and meet our breach-reporting obligations under the GDPR.

Failing to notify a breach when required to do so can result in a significant fine up to 2 per cent of our global turnover. The fine can be combined the ICO's other corrective powers. So, it is important to make sure we have a robust breach-reporting process in place to ensure we detect and can notify a breach, on time; and to provide the necessary details.

5.9 International Transfer

The Data Protection legislation restricts the transfer of personal data to countries outside the EEA, or international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often we carry them out.

5.9.1 Are we Transferring outside of EEA

We are making a restricted transfer if:

- the Data Protection legislation applies to our processing of the personal data we are transferring, and
- we are sending personal data, or making it accessible, to a receiver to which the Data Protection legislation does not apply. Usually because they are located in a country outside the EEA; and
- the receiver is a separate organisation or Data Subject. The receiver cannot be employed by us or by our company. It can be a company in the same group.

Transfer does not mean the same as transit. If personal data is just electronically routed through a non-EEA country but the transfer is actually from one EEA country to another EEA country, then it is not a restricted transfer.

We are making a restricted transfer if we collect information about Data Subjects on paper, which is not ordered or structured in any way, and we send this to a service company located outside of the EEA, to:

- put into digital form; or
- add to a highly structured manual filing system relating to Data Subjects.

Putting personal data on to a website will often result in a restricted transfer. The restricted transfer takes place when someone outside the EEA accesses that personal data via the website.

If we load personal data onto a UK server which is then available through a website, and we plan or anticipate that the website may be accessed from outside the EEA, we should treat this as a restricted transfer.

5.9.2 Is it to a country outside the EEA?

The EEA countries consist of the EU member states and the EFTA States.

The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

The EFTA states are Iceland, Norway and Liechtenstein. The EEA Joint Committee has made a decision that the GDPR applies to those countries and transfers to those countries are not restricted.

5.9.3 General Considerations

Before making a restricted transfer, we must consider whether we can achieve our aims without actually sending personal data.

If we make the data anonymous so that it is never possible to identify Data Subjects (even when combined with other information which is available to receiver), it is not personal data. This means that the restrictions do not apply, and we are free to transfer the anonymised data outside the EEA.

To provide a secure transfer outside the EEA, all employees must work through the following questions, in order and confirm with the DPO. (If by the last question, we are still unable to make the restricted transfer, then it will be in breach of the Data Protection legislation.

- Has the EU Commission made an ‘adequacy decision’ about the country or international organisation?
- If we are making a restricted transfer, then we need to know whether it is covered by an EU Commission “adequacy decision”.
- This decision is a finding by the Commission that the legal framework in place in that country, territory or sector provides ‘adequate’ protection for Data Subjects’ rights and freedoms for their personal data.
- Adequacy decisions made prior to GDPR, remain in force unless there is a further Commission decision which decides otherwise. The Commission plans to review these decisions at least once every four years.
- If it is covered by an adequacy decision, we may go ahead with the restricted transfer. Of course, we must still comply with the rest of the GDPR.

5.9.4 What if there is no adequacy decision?

If there is no 'adequacy decision' about the country, territory or sector for our restricted transfer, we must then find out whether we can make the transfer subject to 'appropriate safeguards', which are listed in the Data Protection legislation.

These appropriate safeguards ensure that both we and the receiver of the transfer are legally required to protect Data Subjects' rights and freedoms for their personal data.

If it is covered by an appropriate safeguard, we may go ahead with the restricted transfer. Of course, we must still comply with the rest of the Data Protection legislation.

Each appropriate safeguard is set out below:

1. A legally binding and enforceable instrument between public authorities or bodies
2. Binding corporate rules
3. Standard Data Protection clauses adopted by the EU Commission
4. Standard Data Protection clauses adopted by a supervisory authority and approved by the Commission.
5. An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA
6. Certification under an approved certification mechanism together with binding and enforceable commitments of the receiver outside the EEA
7. Contractual clauses authorised by a supervisory authority
8. Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the Data Subjects whose personal data is transferred, and which have been authorised by a supervisory authority

If it the restricted transfer is not covered by appropriate safeguards, then we need to consider if the restricted transfer covered by an exception.

If we are making a restricted transfer that is not covered by an adequacy decision, nor an appropriate safeguard the Data Protection Legislation, then we can only make that transfer if it is covered by one of the 'exceptions' identified in the Data Protection legislation.

The Trust should only use these as true 'exceptions' from the general rule that we should not make a restricted transfer unless it is covered by an adequacy decision or there are appropriate safeguards in place.

If it is covered by an exception, we can go ahead with the restricted transfer. Of course, we must still comply with the rest of the GDPR.

Each exception is set out below:

- **Exception 1**. The Data Subject has given his or her explicit consent to the restricted transfer.
- **Exception 2**. We have a contract with the Data Subject. The restricted transfer is necessary for us to perform that contract.
- **Exception 3**. We have (or are we entering into) a contract with a Data Subject which benefits another Data Subject whose data is being transferred. That transfer is necessary for us to either enter into that contract or perform that contract.
- **Exception 4**: We need to make the restricted transfer for important reasons of public interest.

- **Exception 5**: We need to make the restricted transfer to establish if we have a legal claim, to make a legal claim or to defend a legal claim.
- **Exception 6**: We need to make the restricted transfer to protect the vital interests of a Data Subject. He or she must be physically or legally incapable of giving consent.
- **Exception 7**: We are making the restricted transfer from a public register.
- **Exception 8**: We are making a one-off restricted transfer and it is in our compelling legitimate interests.

5.10 Exemptions

5.10.1 General Overview

Most of the exemptions that were in the Data Protection Act 1998 (the 1998 Act) are included as exceptions built in to certain Data Protection legislation provisions or exemptions Data Protection Act 2018 (the DPA 2018).

The 'domestic purposes' exemption in the 1998 Act is not replicated. This is because the Data Protection legislation does not apply to personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity.

If we used to rely on certain exemptions under the 1998 Act, the things we are exempt from may have changed slightly under the new Data Protection legislation.

In some circumstances, the DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, we may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain GDPR provisions.

The exemptions in the DPA 2018 can relieve us of some of our obligations for things such as:

- the right to be informed;
- the right of access;
- dealing with other Data Subject rights;
- reporting personal data breaches; and
- complying with the principles.

Some exemptions apply to only one of the above, but others can exempt us from several things.

Some things are not exemptions. This is simply because they are not covered by the Data Protection Legislation. Here are some examples:

- **Domestic purposes** – personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside the GDPR's scope. This means that if we only use personal data for such things as writing to friends and family or taking pictures for our own enjoyment, we are not subject to the GDPR.

- **Law enforcement** – the processing of personal data by competent authorities for law enforcement purposes is outside the GDPR's scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the DPA 2018. See our Guide to Law Enforcement Processing for further information.
- **National security** – personal data processed for the purposes of safeguarding national security or defence is outside the GDPR's scope. However, it is covered by Part 2, Chapter 3 of the DPA 2018 (the 'applied GDPR'), which contains an exemption for national security and defence.

5.10.2 What exemptions are available

The following provide an overview of the "groups of exemptions available. Each case may be considered on an individual basis and agreed with the DPO.

- **Crime, law and public protection**
- **Regulation, parliament and the judiciary**
- **Health, social work, education and child abuse**
- **Finance, management and negotiations**
- **References and exams**
- **Subject access requests – information about other people**
- **Crime and taxation: general**

5.11 Other Key Factors

5.11.1 Retention of data

The Trust will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which they will either be archived or destroyed. This will be done in accordance with the retention periods detailed in the Trust's Records Retention Schedule (within the Records Management policy)

5.11.2 Privacy relating to collection and use of card data for payment transactions

The following is the Trust's position on payments:

The Trust does store Credit/Debit card data for the purpose of taking payments.

All data is stored securely in compliance with the Payment Card Industry Data Security Standard (PCIDSS).

5.11.3 The NHS Care Record Guarantee

The NHS Care Record Guarantee sets out the rules that will govern information held in the NHS Care Records Service. This forms an important part of the public information protection in respect of the NHS Care Records.

The guarantee covers people's access to their own records, controls on others' access, how access will be monitored and policed, options people have to limit access, access in an emergency, and what happens when someone cannot make decisions for themselves.

5.11.4 Training

All Trust staff will be made aware of their responsibilities for Data Protection through generic and specific training programmes and guidance.

6 Implementation

The policy will be made available to Trust staff via the intranet Information Governance - Kwiki, and stored on Kingsdocs

7. Monitoring Compliance

The effectiveness of the policy will be monitored by the Data Protection Officer, Information Governance Manager and the Caldicott Guardian who will regularly report to the Information Governance Steering Group.

Areas of actual and/or perceived risk will be identified and managed through the Trust's risk management procedures.

The Trust's compliance with the Act will be subject to periodic internal and external review via audit, with findings and action plan monitored by the Trust Executive and Board.

8. Associated Documents

8.1 Related documents:

1.1 Records Management Policy

1.2 Patient Records Procedure

1.3 Corporate Records Procedure

1.4 Information Governance Policy

1.5 Confidentiality Code of Conduct

1.6 Data Quality Policy

1.7 Relevant Procedural Documents

- SEL Data Sharing Framework

9. References:

Data Protection Act 2018

Freedom of Information Act 2000

NHS Records Management Code of Practice

NHS Care Records - Confidentiality

NHS Care Record Guarantee

Code of Practice for the Management of Records Section 46

Information Commissioners' Office Website

Appendix 1: Indications of where Personal Data is processed in the Trust

The following list provides an overview of the type of Personal data about a Data Subject which will be processed for various purposes (this is NOT exhaustive):

- General
  - facilitate management decisions
  - detect fraud
  - enable equal opportunities
  - address any health and safety issues
  - activities under contract;

- Staff and volunteers
  - assess his/her application to become an employee
  - allow the Trust to serve its duties, rights and obligations to the employee, mainly for HR, admin, regulatory or payroll;

- Patients
  - process his/her referral and assess suitability for treatment
  - facilitate the on-going treatment process
  - liaise with care partners to facilitate the treatment process
  - facilitate research and teaching – in certain circumstances only
  - allow the Trust to serve its duties, rights and obligations to patients, principally for admin, regulatory and/or legal purposes;

- for students
  - assess any application for enrolment
  - administer student fees and other payments
  - administer exams or facilitate the certification of exam results
  - administer the student/Trust relationship so that the Trust may properly carry out its duties, rights and obligations.

- For visitors / passers-by
  - CCTV images
  - Social Media
  - Car Parking

This list is not exhaustive and merely a guide as there may be other purposes for which personal information can be used legally.

Appendix 2: What privacy information should we provide to Data Subjects?

The table below summarises the information that we must provide.

What information do we need to provide?	Personal data collected from Data Subjects	Personal data obtained from other sources
The name and contact details of our organisation	✓	✓
The name and contact details of our representative	✓	✓
The contact details of our Data Protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to Data Subjects in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether Data Subjects are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

Appendix 3: Checklist for the review and approval of the Data Protection Policy

To be completed by the policy author and submitted with the policy, and an equality impact

Policy title: Data Protection Policy

assessment, to King's Executive for ratification.

	Yes/no/ Unsure/Not applicable	**Comments**
Front page:		
1. Is the title clear and unambiguous?	Yes	
2. Is the trust logo correct?	Yes	
3. Are all the following details present: • Version and version date • Ratified by and date ratified • Author/s (name and job title) • Responsible committee or director • Date policy comes into effect • Review date • Target audience	 Yes Yes Yes Yes Yes Yes Yes	
Document history:		
4. Is it clear what, if any, document this policy replaces?	Yes	
5. Is the location of the document specified?	Yes	
6. Is the distribution list provided?	Yes	
Policy requirements:		
7. Does the policy follow King's corporate identity guidelines, i.e. language concise and clear, is text in Frutiger, Tahoma or Arial and at least 12pt font, are paragraphs numbered?	Yes	
8. Is there a clear aim including the justification for the policy, how it links with trust priorities and how it integrates with or supersedes any existing policy/ies?	Yes	
9. Is the scope of the policy clear (what is included & excluded)?	Yes	
10. Are all unclear terms defined (or included in a glossary)?	Yes	
11. Is there a dissemination plan?	Yes	

		Yes/no/ Unsure/Not applicable	Comments
12.	Is there an implementation plan, including training and/or support implications?	Yes	
13.	Is it clear how compliance with the policy will be monitored?	Yes	
14.	Has the appropriate consultation taken place?	Yes	
15.	Have appropriate trust groups/committees endorsed the policy?	Yes	
16.	Is an equality impact assessment included?	Yes	
17.	Are references and identification of related documents included?	Yes	

Appendix 4: Equality impact assessment for the Data Protection Policy – initial screening

Service/Function/Policy	Directorate / Department	Assessor(s)	New or Existing Service or Policy?	Date of Assessment
Policy	Operations	Jo Downing IG Manager	Existing – reviewed and updated	16/03/2017

1.1 Who is responsible for this service / function / policy? SIRO

1.2 Describe the purpose of the service / function / policy? Who is it intended to benefit? What are the intended outcomes?

This policy sets out the approach taken within the Trust to work within the Data Protection Act 1998.

1.3 Are there any associated objectives? E.g. National Service Frameworks, National Targets, Legislation

Compliance with Information Governance Toolkit, Monitor and CQC requirements, Records Management NHS Code of Practice

1.4 What factors contribute or detract from achieving intended outcomes?

Successful implementation and compliance with the policy

1.5 Does the service / policy / function / have an impact in terms of race, disability, gender, sexual orientation, age and religion? Details: [see Screening Assessment Guidance]

No

1.6 If yes, please describe current or planned activities to address the impact.

N/A

1.7 Is there any scope for new measures which would promote equality?

No

1.8 Equality Impact Rating [low, medium, high*]:

Low for all

Race □ **Age** □ **Disability** □ **Gender** □ **Religion** □ **Sexual Orientation** □

If you have rated the policy, service or function as having a high impact for any of these equality dimensions, it is necessary to carry out a detailed assessment and then complete section 2 of this form

1.9 Date for next review January 2020