

Appropriate Policy Document

Version:	V1.00
New or Replacement:	New
Policy Number:	
Division & Specialty	Chief Executives Office, Information Governance
Document author(s):	Information Governance Compliance Manager and Data Protection Officer
Contributor(s):	
Executive Sponsor (If Required)	
Title of person responsible for review of document (e.g. Deputy Chief Nurse or Trust Lead (If Required))	Information Governance Compliance Manager and Data Protection Officer
Approved By:	Information Governance Group
Date Approved:	November 2022
Review Date:	November 2025

Policy is:	Trust-wide
------------	-------------------

Version History Log

Version	Date Published	Details of key changes
V1.0		New Document.

Contents

Summary	4
1. Purpose	4
2. Scope	4
3. Compliance	5
4. Responsibilities	5
5. Associated Documentation	6
6. Data Processes	6
7. Compliance	11
8. Retention and Erasure Policies	14
9. APD Review	14
10. Implementation, Monitoring and Review.....	14
Monitoring Compliance.....	14
Equality and Health Inequality Impact Assessment Tool.....	15
Referenced Documents and Metadata.....	17
Signature Sheet	18

Equality, Diversity and Inclusion

Corporate Policy Statement

The United Lincolnshire Hospitals NHS Trust is committed to promoting equality and diversity in all its activities to promote inclusive services, processes, practices and culture. This commitment is articulated in our equality objectives for 2022-2025 [Our equality objectives - United Lincolnshire Hospitals \(ulh.nhs.uk\)](#)

This policy reflects the Trust vision, values and behaviours and supports employees in working for the benefit of patient care. It takes account of the provisions outlined in the Equality Act 2010 to ensure no individual receives less favourable treatment on the grounds of age, disability, sex, race, gender reassignment, sexual orientation, religion and belief, marriage/civil partnership and pregnancy/maternity.

Alongside being committed to a proactive delivery of the Equality Act 2010, the Trust proudly seeks to embody the duties of the Public Sector Equality Duty (2011) in all its activity by:

- 1) Eliminating unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- 2) Advancing equality of opportunity between people who share a protected characteristic and those who do not.
- 3) Fostering good relations between people who share a protected characteristic and those who do not.

We recognise high quality NHS patient care benefits by having a diverse community of staff who value one another and realise the contribution they can make to achieving excellence in rural healthcare.

Summary

This policy has been developed by United Lincolnshire Hospitals NHS Trust to meet the requirement in the Data Protection Act (DPA) 2018. The act outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions to cover these processing activities.

This document demonstrates that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (UK GDPR) Article 5 principles. It includes our retention policies with respect to this data. (See Schedule 1 Part 4).

The APD complements our general record of processing under Article 30 of the UK General Data Protection Regulations (GDPR) and provides SC and CO data with further protection and accountability as well as the Trust's privacy notice.

In line with the legal requirements, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

1. Purpose

- 1.1. This purpose of this policy is to meet the above legal requirement.
- 1.2. The policy sets out the Trust's requirements for compliance with its obligations under the Data Protection Act (DPA) 2018, the General Data Protection Regulation (UK GDPR), and associated laws and best practice and the Caldicott Principles.

2. Scope

- 2.1. This policy covers personal data held and processed by United Lincolnshire Hospitals NHS Trust. Personal data is recorded information from which a living person can be identified, either from the data alone, or when combined with other data that is or may become available to the recipient of the data.
- 2.2. This policy covers personal data about service users, carers, applicants, students and staff (both present and past) and third parties. It includes pseudonymised data but not anonymised data. It applies to all personal data, whether held on premise, cloud, on a portable device or by third parties. It applies to information held electronically and on paper.
- 2.3. This policy covers the Trust's requirements for data protection, whether it is the Data Controller or Data Processor, and where the Trust works in partnership with other organisation(s) as joint Data Controller, for example, to achieve seamless or integrated care for patients or service users.

- 2.4. This policy is applicable to all Trust employees, Non-Executive Directors, students, and contractors and third parties who work for or on behalf of the Trust and who have access to Trust information assets.

3. Compliance

This policy complies with the legislation, standards, guidelines, codes of conduct, and any other relevant document listed in the Referenced Documents' section.

4. Responsibilities

- 4.1. **The Chief Executive** has ultimate responsibility for ensuring that mechanisms are in place for the overall implementation, monitoring and revision of policy.
- 4.2. Senior Information Risk Officer (SIRO) will oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance Framework.
- 4.3. **The Caldicott Guardian** is responsible at Board level for ensuring Trust policies and processes are in line with national and local policies and these are implemented/ upheld. The Caldicott Guardian also has the added responsibility for protecting the confidentiality of patient and service user information and ensuring appropriate information sharing policies are upheld.
- 4.4. **Divisional Directors** are responsible for implementation of the policy within their own spheres of management and must ensure that:
 - All new and existing staff have access to and are informed of the policy.
 - Ensure that local written procedures support and comply with the policy Ensure the policy is reviewed regularly.
 - Staff training needs are identified and met to enable implementation of the policy.
- 4.5. **The Head of Information Governance/ The Data Protection Officer (DPO)** has a duty to ensure the Trust complies with data protection legislation and Information Governance policies and guidance. Their responsibilities include: Informing and advising organisations about complying with General Data Protection Regulation (UK GDPR) and other data protection legislations Monitoring compliance with UK GDPR and data protection laws with the support of IG Manager – including staff training and internal audits; Advising on and monitoring data protection impact assessments; Cooperating with the ICO.
- 4.6. **All Trust staff** are responsible for ensuring that they:
 - Are responsible to work within the content of this document and relevant policies.
 - Work within, and do not exceed, their own sphere of competence.

5. Associated Documentation

- Information Governance Policy
- Data Protection Policy
- Data Protection Impact Assessment Template
- Freedom of Information policy
- Privacy Notice

6. Data Processes

Under the Data Protection Act 2018, the Trust primarily processes data under the legal basis of, the performance of a task carried out in the public interest and in exercising our official authority. This means that it is necessary for us to process data for those purposes.

Additionally, other alternative conditions may be applicable where the above justification is not available for example, in the event of a life or death situation such as to prevent harm being caused by a patient or service user.

We have set out in the below table a description of all the ways we use personal data, and the legal bases we rely on to do so.

Purpose/Activity	Type of Data	Lawful basis for processing including basis of legitimate interest
Direct Care	a) Identity b) Contact c) Special Categories such as health information	All Health and Adult Social Care providers are subject to the statutory duty under Section 251B of the Health and Social Care Act 2012 to share personal data about patient for their direct care. UK GDPR Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. GDRP Article (2) (h) Processing is necessary for the purposes of preventative or occupational medicine for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or management of health or social cares systems and services on the basis of Union or Member State law or a contract with a health professional.
Respond to a request under Freedom of Information, enquiries, complaints	a) Identity b) Contact	UK GDPR Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller.
Respond to a request under Data Protection Act or General Data Protection Regulation	a) Identity b) Contact c) Special Categories such as health information	UK GDPR Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller.
Safeguarding	a) Identity b) Contact c) Special Categories such as health information	Health and Social Care organisations have a duty to make enquiries where an individual is experiencing or is at risk of abuse or neglect. UK GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller.

		UK GDPR Article 9 (2) (b) Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of social protection law in so far as it is authorised by Union or Member State Law.
To investigate and respond to a complaint (including whistleblowing)	a) Identity b) Contact c) Special Categories	UK GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. UK GDPR Article 9 (2) (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
Commissioning and Planning Purposes	a) Identity b) Contact c) Special Categories	Data is sent to the commissioners of our services who pay us for providing services. We are also required to report to National bodies on our activities and performance. United Lincolnshire Hospitals NHS Trust undergoes external audit by the Audit Commission or other professional bodies given the legal authority to carry out audits. These audits may involve reviewing information in patient records to ensure accuracy, completeness and the competency of Trust staff. NHS digital establishes most national and local flows of personal data. These flows do not operate based on consent for confidentiality or data protection purposes. Article 6 (1) (c) Processing is necessary for compliance with a legal obligation. Article 6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 9 (2) (h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
Research	a) Identity b) Contact c) Special Categories	For research purposes, the common law duty of confidentiality must still be met through consent. Consent is still needed for people outside the care team to access and use service user personal data for research, unless there is Section 251B of the Health and Social Care Act 2012 support or the data is anonymised (no longer identifiable). This

		<p>includes encryption techniques, such as pseudonymisation (using special codes).</p> <p>Article 6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p> <p>Article 9 (2) (j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).</p>
<p>Employment Purpose (staff and volunteers)</p>	<p>a) Identity b) Contact c) Special Categories</p>	<p>For employment purposes the below lawful reasons for lawful processing will apply, this includes special categories of data such as health data for employment purposes.</p> <p>Article 6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p> <p>Article 9 (2) (b) Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of social protection law in so far as it is authorised by Union or Member State law.</p> <p>Personal data processed in relation to the Disclosure and Barring Service (DBS checks) falls under the UK GDPR (Article 10) and the provision of Safeguarding Vulnerable Groups Act 2006.</p>
<p>Surveys</p>	<p>(a) Identity (b) Contact (c) Special Categories</p>	<p>In some cases, the Trust may commission a survey for a specific reason, such as monitoring improvement in care; this may be commissioned with explicit consent of those taking part or on another legal basis, e.g. patient satisfaction surveys.</p> <p>The Trust may contract third party organisations to work on survey development and analysis on its behalf. In such circumstances, participants will be notified in advance of their data being gathered.</p> <p>UK GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller.</p> <p>UK GDPR Article 9 (2) (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.</p>

<p>Processing of data relating to criminal conviction</p>	<p>(c) Special Categories</p>	<p>The Trust may sometimes process data relating to criminal conviction for the recruitment /employment related purposes including Human Resource (HR).</p> <p>The Trust ensures that personal data relating to criminal conviction that it collects from employees are used only for employment related purposes or where there is a statutory obligation to share those data with regulatory bodies (e.g. courts or police).</p> <p>Legal basis for processing data relating to criminal conviction in the area recruitment and employment. The Trust ensures that the lawfulness of processing of special categories of personal data and criminal convictions data 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 under <i>UK GDPR Article 9 (2) (b)</i> is permitted under <i>DPA Section 10(1) (c)</i>: The processing is necessary for employment purposes.</p> <p>Additional conditions for processing data relating to criminal conviction data. <i>DPA Schedule 1, Part 3</i> sets out the additional conditions which must be met when processing data relating to criminal conviction data. Therefore, in line with clause 29 of this Schedule, the Trust relies on the consent of the data subject/staff in other to process their personal data relating to criminal conviction data by virtue of employment.</p>
<p>Statutory Disclosure</p>	<p>May be legally required to share personal data concerning health with law enforcement and regulatory bodies such as: NHS England, Police, Courts of Justice, HMRC, Medico-Legal, NHS Counter Fraud, and Health Service ombudsman</p>	<p>In some circumstances the for the purposes of:</p> <ul style="list-style-type: none"> - Safeguarding, investigation, prevention or detection of crime; - Apprehension or prosecution of offenders; - The assessment or collection of any tax or duty or, of any imposition of a similar nature; - Providing medical reports in connection with legal action.
<p>Statutory Collection</p>	<p>Personal data</p>	<p>Sharing of personal data concerning health with NHS Digital for the purpose of National Data collections/ extraction</p>

7. Compliance

Accountability principle

The Trust maintains a record of processing activities under Article 30 of the UK GDPR and has suite of data protection policies.

The Trust carries out Data Protection Impact Assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests and have a process for review and approval.

The Trust has appointed a Data Protection Officer (DPO) for monitoring and providing assurance on the Trust compliance with Data Protection/ GDPR principles.

The Trust will work to ensure:

- DPO function has sufficient resource (expert and administrative) to: Ensure processes are in place so that records are kept of personal data processing activities through data flow mapping.
- Instil the requirement of completion of Data Protection Impact Assessments (DPIA).
- Will provide advice and monitoring of the Trust's personal data handling.
- Have in place processes to ensure personal data is collected, used or handled in a way compliant with data protection law.

Principle (a): lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to data subjects.

The Trust will:

- Ensure personal data is only processed where a lawful basis has been identified and where processing is otherwise lawful.
- Process personal data fairly and ensure data subjects are not misled about the purposes of any processing- [see Privacy Notice.](#)
- Embed a process for the completion and assessment of DPIAs where changes to processing take place. For details on the Trust, process and templates visit the IG Pages on the intranet.
- Ensure data subjects have access to full privacy information so that any processing of personal data is transparent- [see Privacy Notice.](#)

Principle (b): purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes for the primary purpose of health care provision/ direct care, and not further processed in a manner incompatible with the purpose.

The Trust will:

- Collect personal data for specified, explicit and required purposes and will inform data subjects what those purposes are in a privacy notice- [see Privacy Notice](#).
- Not use personal data for purposes incompatible with the purposes for which it was collected or where a statutory basis exists.
- Ensure any changes to the processing of data are considered through a thorough DPIA process.

Principle (c): data minimisation

The Trust will look to ensure personal data (staff and patient) shall be adequate, relevant and limited to: what is necessary in relation to the purposes for which they are processed.

The Trust will:

- Only collect and use the minimum personal data that is needed for the purposes for which it is collected. 'Data minimisation'
- Ensure processes are in place to have assurances that the personal data we collect is adequate and relevant.

Principle (d): accuracy

The Trust shall look to ensure personal data shall be accurate and where necessary, kept up to date.

The Trust will:

- Ensure processes are in place so that personal data is accurate and kept up to date where necessary. For example checking of details at reception areas when patients attend clinic.
- Carry out data quality exercises as part of standard practice. For example data checking against national systems available to the NHS.

- Include data accuracy clauses within agreements with other organisations where data sharing takes place.
- Have processes in place to manage the rectification of data errors in records.

Principle (e): storage limitation

The Trust shall look to ensure data be kept in a form which permits identification of data subjects no longer than necessary (or required legally) for purposes for which the personal data is processed.

The Trust will:

- Keep personal data in identifiable form for as long as necessary for purposes for which it is collected or where we have a legal obligation to do so. In the NHS we are required to retain data for legal medical purposes and evidence of decision making so this may not be possible.
- A programme will exist so data shall be reviewed and deleted in line with [National Department of Health](#) guidance on the retention of health records as appropriate.

Principle (f): integrity and confidentiality (security)

The Trust shall look to ensure personal data be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using the appropriate technical or organisational measures.

The Trust will:

- Ensure there are appropriate technical and organisational measures in place to protect personal data. This includes:
 - Provide regular training to staff basis in relation to Data Protection and confidentiality.
 - Restrict access to personal data to only those individuals who need access for their role.
 - Carry out due diligence on third party organisations we work with who may be involved in the processing of personal data, and ensure appropriate contracts are in place.
 - Having appropriate policies and procedures in place.

8. Retention and Erasure Policies

- 8.1. We will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal or reporting requirements.
- 8.2. To determine the appropriate retention period for personal data, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which the data was processed and whether we can achieve those purposes through other means, and the applicable legal requirements will be considered.
- 8.3. Records held by ULHT will be kept for the duration specified by national guidance from Department of Health found in the Records Management: NHS code of practice for health and social care, supplemented by the Trusts Records Management Policy and Retention schedule.

9. APD Review

- 9.1. This Policy will be formally reviewed every three years or, when changes in legislations, statutory requirements necessitate earlier review.
- 9.2. This Policy may also be reviewed and amended at any time if it is considered amendments are required to ensure the Policy is up to date and accurate.

10. Implementation, Monitoring and Review

This document will be published on the Trust internet to fulfil its public facing requirement.

No specific training is required- this is a statutory information document.

Monitoring Compliance

Minimum requirement to be monitored – monitoring against standards set out in policy	Process for monitoring e.g. audit	Responsible individuals/ group/ committee	Frequency of monitoring/ audit/ reporting	Responsible individuals/ group/ committee for review of results and determining actions required
Publication on intranet and website	N/A	Information Governance Group	N/A	IG Compliance Manager & DPO

Equality and Health Inequality Impact Assessment Tool

This tool has been developed by the Equality, Diversity and Inclusion Leads for use in the NHS Provider organisations in Lincolnshire. The tool is designed to ensure due regard is demonstrated to the Equality Act 2010, the Public Sector Equality Duty and potential health inequalities are also identified and addressed (as outlined in the Health and Social Care Act). Please complete all sections below. Instructions are in *italics*. Support can be found at <http://ulhintranet/equality-and-diversity>.

A. Service or Workforce Activity Details	
1. Description of activity	<i>Production of an Appropriate Policy document</i>
2. Type of change	New
3. Form completed by	<i>Information Governance Compliance Manager</i>
4. Date decision discussed & proposed	<i>10/11/2022</i>
5. Who is this likely to affect?	Service users <input checked="" type="checkbox"/> Staff <input checked="" type="checkbox"/> Wider Community <input type="checkbox"/> If you have ticked one or more of the above, please detail in section B1, in what manner you believe they will be affected.
B. Equality Impact Assessment	
Complete the following to show equality impact assessment considerations of the decision making to ensure equity of access and to eliminate harm or discrimination for any of the protected characteristics: age , disability , gender reassignment , marriage and civil partnership , pregnancy and maternity , race , religion or belief , sex , sexual orientation . Further, please consider other population groups which are at risk of health inequality and can include, but not be limited to, people who are; living in poverty / deprivation, geographically isolated (e.g. rural), carers, agricultural workers, armed forces, migrants, homeless, asylum seekers/refugees, surviving abuse, in stigmatised occupations (e.g. sex workers), use substances etc. Please ensure you consider the connections (intersectionality) between the protected characteristics and population groups at risk of health inequality (e.g. it is recognised that older men from a BAME background, with one or more comorbidities and living in deprivation are more at risk of a poorer outcome if they contract CV-19).	
1. How does this activity / decision impact on protected or vulnerable groups? (e. g. their ability to access services / employment and understand any changes?) Please ensure you capture expected positive and negative impacts.	No impact.
2. What data has been/ do you need to consider as part of this assessment? What is this showing/ telling you?	Patient data / workforce data Special category data
C. Risks and Mitigations	
1. What actions can be taken to reduce / mitigate any negative impacts? (If none, please state.)	N/A
2. What data / information do you have to monitor the impact of the decision?	N/A
D. Decision/Accountable Persons	
1. Agreement to proceed proposed?	Yes
2. Any further actions required?	<i>Publication to intranet and website.</i>
3. Name & job title accountable decision makers	Senior Information Risk Owner
4. Date of decision	<i>10/11/2022</i>
5. Date for review	.

Purpose of the Equality and Health Inequality Assessment tool

- The NHS in Lincolnshire has a legal duties under the Equality Act 2010, Public Sector Equality Duty 2011 and the Health and Social Care Act 2012 to demonstrate due regard in all decision making, for example, when making changes to services or workforce practices, to ensure access to services and workforce opportunities are equitable and to avoid harm and eliminate discrimination for each of the protected characteristics and other groups at risk of inequality.
- Within the guidance toolkit there are also some examples of decisions this tool has been used on in other organisations and the impacts they have identified.

Checklist

- Is the purpose of the policy change/decision clearly set out?
- Have those affected by the policy/decision been involved?
- Have potential positive and negative impacts been identified?
- Are there plans to alleviate any negative impact?
- Are there plans to monitor the actual impact of the proposal?

This form is based on a template produced by Cambridge University Hospitals NHS Trust and used with their kind permission. FINAL Trust Leadership Team approved for use 01.04.2021

Referenced Documents and Metadata

References

- The Data Protection Act 2018
- General Data Protection Act (EU 2016/679)
- Freedom of Information Act 2000
- Human Rights Act 1998

Other Documents

None

Metadata

Appropriate Policy Document

Special Category Data

Legal Basis

Purpose Limitation

Signature Sheet

Names of people consulted about this policy:

Name	Job title	Department

Author(s) confirm that they have collected all the signatures, as listed above, email Corporate Governance at corporate.policies@ulh.nhs.uk

YES / NO

Names of committees which have approved the policy	Approved on
Information Governance Group	November 2022