Lincolnshire Community and Hospitals NHS Group

## Group Appropriate Policy Document

Reference No.: LCHG_P_CoG_08

Version: V1.0

Approved By: Information Governance Group

Date Approved: September 2025

Division and Specialty: Corporate Affairs/Information Governance

Job Title of Author / Reviewer: Head of Information Governance

Job title of Contributors: Data Protection Officer (LCHS) and Information Governance Compliance Manager (ULTH)

Executive Sponsor: Director of Corporate Affairs

Title of Person Responsible for Review of Document: Head of Information Governance

Date Issued: September 2025

Review Date: September 2028

Target Audience: The policy applies to all employees, contractors, consultants, agency staff and board members when acting on behalf of the LCHG.

Distributed Via: LCHS Public Website and ULTH SharePoint

## Version Control Sheet

| Version | Section / Paragraph / Appendix | Version / Description of Amendments | Date | Author / Amended by |
|---|---|---|---|---|
| V1.0 | Not Applicable | To replace<br>ULTH – Appropriate Policy Document (P–80) | September 2025 | Fiona Hobday, Head of Information Governance (ULTH)<br>Kaz Lindfield–Scott, Data Protection Officer (LCHS) |

## Policy Document Statement

| | |
|---|---|
| **Background Statement** | This Appropriate Document describes the system and processes used by Lincolnshire Community Health Services NHS Trust (LCHS) and United Lincolnshire Hospitals Teaching Hospitals NHS Trust (ULHT) hereafter referred to as Lincolnshire Community and Hospitals NHS Group (LCHG – The Group), in its approach to comply with the legal requirements, to 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'). |
| **Key Words** | Appropriate Policy Document, Criminal Offence Data, Data Protection Act, Public Interest, Special Category Data |
| **Responsibilities** | All employees, contractors, consultants, agency staff and Board members when acting on behalf of Group. All information and systems used or managed by Group. Any individual using information or requiring access 'owned' by the Group. |
| **Training** | All staff, including temporary and third-party contractors working on before of Group will have access to training through induction, mandatory or e-learning nodules. |
| **Dissemination** | This policy will be shared with the staff internally by Group Communications the LCHS Public Website and ULTH SharePoint. |
| **Resource Implication** | None. |
| **Consultation** | Internal consultation with senior members of staff within Data Protection and Information Governance, and approval by the Information Governance Group. |
| **Monitoring** | Through regular review of processes, audit and outcome reports. |
| **Equality Statement** | As part of our on-going commitment to promoting equality, valuing diversity and protecting human rights, Lincolnshire Community and Hospitals NHS Group is committed to eliminating discrimination against any individual (individual means employees, patients, services users and carers) on the grounds of gender, gender reassignment, disability, age, race, ethnicity, sexual orientation, socio-economic status, language, |

religion or beliefs, marriage or civil partnerships, pregnancy and maternity, appearance, nationality or culture.

# Contents

# 1. Introduction

This Appropriate Policy Document (APD) sets out how the Group ensures that the processing of Special Category (SC) and Criminal Offence (CO) data complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It outlines the legal basis, safeguards, and governance arrangements in place to protect this sensitive data.

This document has been developed by to meet the requirement in the Data Protection Act (DPA) 2018. 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 UK General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

# 2. Purpose

The purpose of this document is to:

- Demonstrate compliance with Article 5 of the UK GDPR.
- Fulfil the requirement under Schedule 1, Part 4 of the DPA 2018 to have an APD in place.
- Provide transparency and accountability in the processing of Special Category (SC) and Confidential (CO) data.

# 3. Context

The Group processes SC and CO data in the course of delivering its services and fulfilling its legal obligations. This includes data relating to health, ethnicity, criminal records, safeguarding, and legal claims. The processing is carried out in accordance with the principles of data protection and subject to appropriate safeguards.

# 4. Objectives

- To ensure lawful, fair, and transparent processing of SC and CO data.
- To apply appropriate technical and organisational measures to protect data.
- To define roles and responsibilities for data protection compliance.
- To ensure data is retained only as long as necessary and securely disposed of.

# 5. Scope

This policy covers Lincolnshire Community Health Services NHS Trust (LCHS) and United Lincolnshire Hospitals Teaching Hospitals NHS Trust (ULHT) hereafter referred to as Lincolnshire Community and Hospitals NHS Group (LCHG – The Group)

This document covers personal data held and processed by LCHG. 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.

This document covers personal data about patients, carers, applicants, students and staff (both present and past) and third parties. It includes pseudonymised data but not anonymised data and applies to all personal data, whether held on paper, digital on premise, cloud, a portable device or by third parties.

This document covers the Groups requirements for data protection, whether it is the Data Controller or Data Processor, and where the Group works in partnership with other organisation(s) as joint Data Controller, for example, to achieve seamless or integrated care for patients or service users.

This policy is applicable to all Group 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.

## 6. Compliance

In accordance with the accountability principle, The Group maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. We carry out data protection impact assessments where appropriate in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 for law enforcement processing to ensure data protection by design and default.

6.1. Legal Basis

- Special Category Data is processed under Article 9(2) of the UK GDPR and relevant conditions in Schedule 1, Parts 1 and 2 of the DPA 2018.
- Criminal Offence Data is processed under Article 10 of the UK GDPR and Schedule 1, Parts 1, 2, and 3 of the DPA 2018.

6.2. Schedule 1 Conditions

- Part 1: Employment, health, and research (e.g., Paragraphs 1–4).
- Part 2: Substantial public interest (e.g., Paragraphs 6, 8, 10, 18).
- Part 3: Legal claims and judicial acts (e.g., Paragraphs 33, 35).

6.3. Article 10 – Criminal Conviction Data – Processing of CO data is only permitted:

- Under the control of official authority, or
- Where authorised by domestic law with appropriate safeguards.

## 7. Responsibilities

- Senior Information Risk Owner (SIRO) - has overall responsibility for the Groups Information Risk Policy and acts as champion for information risk on the Board.
- Chief Executive has ultimate responsibility for ensuring that mechanisms are in place for the overall implementation, monitoring and revision of policy.
- Caldicott Guardian is responsible for ensuring Trust policies and processes are in line with national and local policies and are implemented/ upheld. The Caldicott Guardian has the added responsibility for protecting the confidentiality of patient information and ensuring appropriate information sharing policies are upheld
- Head of Information Governance/ Data Protection Officer has a duty to ensure the Trust complies with data protection legislation and Information Governance policies and guidance, and acts as a subject matter expert.
- 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.

## 8. Definitions

- Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation.
- Criminal Offence Data: Data relating to criminal convictions, offences, allegations, proceedings, or sentencing.
- Appropriate Policy Document (APD): A document required under the DPA 2018 to demonstrate compliance when processing SC or CO data under certain conditions.

## 9. Data Processes

Under Data Protection, the Group processes data for 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<br>b) Contact<br>c) Special Categories | 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.<br>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.<br>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 heath or social cares systems and services on the basis of Union or Member State law or a contract with a health professional. |
| **To respond to a request under the Freedom of Information Act, enquiries, complaints** | a) Identity<br>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. |
| **To respond to a request under Data Protection Act or the General Data Protection Regulation** | a) Identity<br>b) Contact<br>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<br>b) Contact<br>c) Special Categories such as health information | Local Authorities have a duty to make enquiries where an adult is experiencing or is at risk of abuse or neglect.<br>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<br>b) Contact<br>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.<br>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<br>b) Contact<br>c) Special Categories | Data is sent to the commissioners of our services who pay us for providing our services. We are also required to report to the Department of Health on our activities and performance.<br>The Group 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 Group staff.<br>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.<br>Article 6 (1) (c) Processing is necessary for compliance with a legal obligation.<br>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.<br>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<br>b) Contact<br>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 includes encryption techniques, such as pseudonymisation (using special codes). |

| | | |
|---|---|---|
| | | 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.<br>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). |
| **Employment Purpose (staff and volunteers)** | a) Identity<br>b) Contact<br>c) Special Categories | 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.<br>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.<br>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.<br>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. |
| **Surveys** | (a) Identity<br>(b) Contact<br>(c) Special Categories | In some cases, the Group 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.<br>Group 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.<br>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.<br>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. |
| **Processing of data relating to criminal conviction** | (c) Special Categories | The Trust may sometimes process data relating to criminal conviction for the recruitment /employment related purposes including Human Resource (HR). |

| | | |
|---|---|---|
| | | 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).<br>**Legal basis for processing data relating to criminal conviction in the area recruitment and employment.**<br>The Group 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 *UK GDPR Article 9 (2) (b)* is permitted under *DPA Section 10(1) (c):* The processing is necessary for employment purposes.<br>**Additional conditions for processing data relating to criminal conviction data.**<br>*DPA Schedule 1, Part 3* 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. |
| **Statutory Disclosure** | Trust may be legally required to share personal data concerning health with law enforcements and regulatory bodies such as: NHS England, Police, Courts of Justice, HMRC, DVLA, Medico-Legal, NHS Counter Fraud, and Health Service ombudsman | In some circumstances the for the purposes of:<br>1. Safeguarding, investigation, prevention or detection of crime;<br>2. Apprehension or prosecution of offenders;<br>3. The assessment or collection of any tax or duty or, of any imposition of a similar nature;<br>4. Providing medical reports in connection with legal action. |
| **Statutory Collection** | Personal data | Sharing of personal data concerning health with NHS Digital for the purpose of National Data collections/ extraction |

## 10. Compliance

**Accountability principle**

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

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

The Group has appointed relevant Data Protection Officers (DPO) for monitoring and providing assurance on the Groups compliance with Data Protection/ GDPR principles.

The Group will work to ensure:

1. 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.
2. Instil the requirement of completion of Data Protection Impact Assessments (DPIA).
3. It will provide advice and monitoring of the Trust's personal data handling.
4. Have in place internal processes to ensure personal data is collected, used or handled in a way that is 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:

1. Ensure personal data is only processed where a lawful basis has been identified and where processing is otherwise lawful.
2. Process personal data fairly and ensure that data subjects are not misled about the purposes of any processing-:
   - See ULTH Privacy Notice(s)/
   - See LCHS Privacy Notice(s)
3. 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.
4. Ensure data subjects have access to full privacy information so that any processing of personal data is transparent-
   - See ULTH Privacy Notice(s)/

- See LCHS Privacy Notice(s)

**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:

1. Collect personal data for specified, explicit and required purposes and will inform data subjects what those purposes are in a privacy notice-
   - See ULTH Privacy Notice(s)/
   - See LCHS Privacy Notice(s)
2. Not use personal data for purposes that are incompatible with the purposes for which it was collected or where a statutory basis exists.
3. 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:

1. Only collect and use the minimum personal data that is needed for the purposes for which it is collected. 'Data minimisation'
2. 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:

1. 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.
2. Carry out data quality exercises as part of standard practice. For example data checking against national systems available to the NHS and baseline monitoring against regional partners.

3. Include data accuracy clauses within agreements with other organisations where data sharing takes place.
4. 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:

1. Keep personal data in identifiable form for as long as necessary for the 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.
2. 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:

1. 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.

## 11. Retention and Erasure Policies

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.

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.

Records will be kept for the duration specified by national guidance from Department of Health & Social Care in the Records management: NHS code of practice for health and social care, supplemented by the Trust Records Management policy and Retention schedule.

## 12. Associated Documentation

- P_IG_26_Data_Protection_Policy_v3.pdf (LCHS)
- P_IG_28_Records_Management_Policy_v3.1.pdf (LCHS)
- P_IG_27_Information_Security_Policy_v3.pdf (LCHS)
- P_IG_30_Information_Risk_Policy_v3.pdf (LCHS)
- Security Policy and Strategy (LCHS)
- LCHG-P-CG-03_Incident_Management_Policy.pdf (LCHG)
- Data Protection and Confidentiality Policy (ULTH)
- Information Governance Policy (ULTH)
- Records Management Policy (ULTH)

## 13. References and Other Documentation

- Fair Processing Notice/ Privacy Notice : Lincolnshire Community Health Services NHS Trust (LCHS)
- Fair Processing Notice (ULTH)
- Records Management Code of Practice - NHS Transformation Directorate
- What is special category data? | ICO
- UK General Data Protection Regulation | ICO
- Data Protection Act 2018

## 14. Implementation, Monitoring and Compliance

| **Minimum requirement to be monitored – monitoring against standards set out in policy** | **Process for monitoring**<br>**e.g. audit** | **Responsible individuals/ group/ committee** | **Frequency of monitoring/ audit/ reporting** | **Responsible individuals/ group/ committee for review of results and determining actions required** |
|---|---|---|---|---|
| Monitoring of incidents concerning data breaches of special category data. | Audit | Head of IG/ DPO | Bi-monthly | Information Governance Group |
| Monitoring of DSAR requests received under the purpose of this policy | Audit | Head of IG/ DPO | Bi-monthly | Information Governance Group |

## Review of Document

This policy will be due for review in 3 years' time. An earlier review may be warranted if one or more of the following occurs:

- As a result of regulatory or statutory changes or developments.
- Due to the findings or outcomes from incidents and root cause analysis.
- Or any other relevant or compelling reason.

# Appendix A – 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 **bold**
Email for all correspondence: email to lhnt.edifirst@nhs.net

## Service or Workforce Activity Details

| | |
|---|---|
| Description of activity | A document required under the DPA 2018 to demonstrate compliance when processing SC or CO data under certain conditions. |
| Type of change | adjust existing |
| Form completed by | Kaz Lindfield-Scott, Data Protection Officer, LCHS |
| Date decision discussed & agreed | 2 July 2025 |
| Who is this likely to affect? | Service users x Staff x Wider Community x<br><br>*If you have ticked one or more of the above, please detail in section B1, in what manner you believe they will be affected.* |

## 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, 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).

| | |
|---|---|
| How does this activity / decision impact on protected or vulnerable groups? (e. g. their ability to access services / employment and understand any changes?)<br>Please ensure you capture expected positive and negative impacts. | A document required under the DPA 2018 to demonstrate compliance when processing SC or CO data under certain conditions. |
| What data has been/ do you need to consider as part of this assessment? What is this showing/ telling you? | Personal Identifiable Information, Sensitive' Special Category data and Criminal Offence data, |

## Risks and Mitigations

| | |
|---|---|
| What actions can be taken to reduce / mitigate any negative impacts? (If none, please state.) | None. |
| What data / information do you have to monitor the impact of the decision? | Personal Identifiable Information, Sensitive' Special Category data and Criminal Offence data, |

## Decision/Accountable Persons

| | |
|---|---|
| Endorsement to proceed? | Yes. |
| Any further actions required? | No. |
| Name & job title accountable decision makers | Information Governance Group Members as named on the terms of reference. |
| Date of decision | 10 September 2025 |
| Date for review | September 2028 |

## 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. Draft NHS Lincolnshire EDI System 2.1

## Signature Sheet

Names of people consulted about this policy:

| Name | Job title | Department |
|---|---|---|
| Fiona Hobday | Head of Information Governance | ULTH |
| Kaz Lindfield – Scott | Data Protection Officer | LCHS |

| | |
|---|---|
| Author(s) confirm that they have collected all the signatures, as listed above, email Corporate Governance at ulth.corporate.policies@nhs.net (ULTH) / lhnt.policies@nhs.net (LCHS) | **YES** |

| Names of committees which have approved the policy | Approved on |
|---|---|
| Information Governance Group | 10 September 2025 |