Data protection policy

Introduction and scope

We have a statutory duty to meets our obligations as set out within data protection legislation as we process personal data when conducting our business.

Aim

This policy explains how we will meet our obligations under data protection legislation.

Scope

This policy applies to:

- all personal data that we process, in any format
- any individual processing personal data that we hold

Key definitions

Data Protection Legislation: UK General Data Protection Regulation (“UK GDPR”), Data Protection Act 2018 (“DPA 2018”), Privacy and Electronic Communications Regulations 2003, and any other relevant law concerning the processing of personal data.

Data: information processed by automated or non-automated means, including structured files that are accessible by specific criteria.

Personal data: any information that can, either directly or indirectly, identify a living person. Identifiers include:

- name
- address
- date of birth
- postcodes
- unique identification numbers
- location data
- online identifiers (such as an IP address)
- pseudonymised data
- information relating to a person's social or economic status

Special category data: personal data consisting of information relating to:

- race or ethnicity
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership or affiliation
- physical or mental health or condition
- biometric and, or genetic data
- sex life or sexual orientation

Criminal convictions data: personal data relating to:

- the alleged commission of offences by the data subject, or
- proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Processing: any action on personal data, such as collection, use, storage, sharing, or destruction (whether by automated or manual means).

Data subject: the individual whose data is being processed.

Controller: the person or organisation that decides (either alone or jointly with others) how and why personal data is processed.

Processor: any person or organisation that processes data on behalf of the controller.

Law enforcement processing: processing personal data for the purpose of:

- the prevention, investigation, detection or prosecution of criminal offences, or
- the execution of criminal penalties, including protecting and preventing threats to public security

The six data protection principles

We shall adhere to the six principles of data protection, which are:

1. fairness, lawfulness and transparency: personal data shall be processed fairly and lawfully and in a transparent manner
2. purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with that purpose
3. data minimisation: personal data shall be adequate, relevant and limited to what is necessary for the purpose
4. accuracy: personal data shall be accurate and, where necessary, kept up to date
5. storage limitation: personal data shall be kept in a form that permits identification for no longer than necessary

6. security: personal data shall be processed in a manner that ensures appropriate security

Additionally, we will ensure compliance with the accountability principle, meaning we keep records to show we're meeting these standards.

Our responsibilities

We will:

- register with the information commissioner's office and pay the annual statutory data protection fee. Our data protection registration number is Z8397628
- have policies and processes in place to support us to meet our data protection obligations
- employ specialist staff with specific responsibility for providing support and guidance
- ensure staff processing personal data understand that they are responsible for complying with data protection legislation and are appropriately trained

Data protection officer (DPO)

We will have in place a DPO.

The DPO supports us to meet our obligations under data protection legislation. The role, which is a statutory requirement will:

- monitor our ongoing compliance
- provide advice and guidance on all data protection matters
- act as a point of contact for data subjects
- investigate and respond to complaints concerning data protection (as defined in our complaints policy), aiming to provide a response within one calendar month. Where it is not possible to provide a response within this timeframe, regular updates will be provided.
- act as a single point of contact for the information commissioner's office (ICO), including consulting the ICO on high-risk processing activities that we cannot fully reduce and manage

Data Protection roles and responsibilities

- senior information risk owner (siro): owns information risk management at director level and is responsible for leading and fostering a culture that values, protects and uses information responsibly
- Caldicott guardians: ensure compliance with both data protection legislation and the Caldicott Principles where personal data is processed for health and social care purposes
- head of information assurance: manages the information assurance strategy and assists with in the identification, management and implementation of information risk
- information governance manager: fulfils the role of data protection officer and manages a team who deliver information governance support and guidance, ensuring that staff are aware of their data protection responsibilities

- information assurance team: provides advice, guidance and training on data protection, information security and records management
- information asset owners (iao): oversee specific information assets and are key decision makers across information they are responsible for
- managers: ensure that the requirements of this policy are integrated into service procedures and that staff comply with all policies relevant to their role
- staff: ensure they process information in line with the requirements of this policy, undertake mandatory annual training and understand that failure to do so could result in disciplinary action

Records of processing activity

We will maintain written records of our data processing activities, including:

- an information asset register
- a directory of privacy notices
- a directory of retention schedules
- policies detailing technical and organisational security measures in place to protect personal data

We will also have specific policies for processing special category data, criminal conviction data and law enforcement data.

Privacy notices

We will provide privacy notices to individuals about how personal data about them is used. They will be in plain English, and available upon request and free of charge.

Data Protection Impact Assessment (DPIA)

For high-risk activities, such as large-scale processing of special category data or monitoring public spaces, we will conduct a DPIA to assess and address privacy risks.

Staff will consult with the Information Assurance team at an early stage to identify DPIA requirements.

The DPO shall be consulted on all DPIAs.

Security of personal data

We will implement organisational and technical controls that help reduce the risk of personal data breaches.

We will record and investigate all personal data breaches.

Where it is determined that a breach results in a risk to the rights and freedoms of an individual(s) we will aim to report the breach to the Information Commissioner's Office within 72 hours of becoming aware.

Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) we shall inform the individual(s) without undue delay.

We will make security policies and procedures available to all staff.

Contracted services

Contracts will include measures to ensure third parties handling personal data on our behalf do so in accordance with data protection legislation.

We will only supply personal data to third parties for the agreed purposes as set out in the contract. Third parties will not be permitted to use or disclose personal data for any other reason.

We will ensure that before we share personal data with a third party as part of a contract, appropriate security controls are in place.

Sharing personal data

We will only share personal data where necessary and where the law allows it.

We will ensure that adequate security is in place to protect personal data when we share it with another organisation.

We shall ensure that information sharing arrangements are appropriately documented.

The Information Assurance Team will provide staff with guidance on:

- sharing personal data in the context of systematic sharing and
- sharing in ad-hoc, one off circumstances

NHS national data opt-out

We will comply with the NHS national data opt-out, allowing individuals to opt-out of their data being used for research and planning purposes.

We will only apply the requirements of the national data opt-out to:

- personal data that identifies an individual in receipt of adult care services and
- so far as that data relates specifically to their health, care or treatment

Individual rights

We will have processes in place to support individuals who wish to exercise their rights in respect of their personal data.

We will respond to any request to exercise individual rights within one calendar month.

Training and awareness

We will provide mandatory annual data protection training to all staff handling personal data.

Staff will maintain a good awareness of data protection.

Additional training will be provided where appropriate.

Surveillance camera systems

We will publish a surveillance camera system policy and supporting guidance for all staff. This will set out our commitment to meet our data protection and wider legal obligations when using such systems.

We will ensure that any use of surveillance camera systems is necessary and proportionate to achieve its objective. Any introduction of surveillance camera systems for a new purpose will be subject to a Data Protection Impact Assessment prior to being used.

International transfers

We will not transfer personal data outside the United Kingdom, unless required by law or with appropriate safeguards in place.

Information Commissioner's Office

We will comply fully with all requests from the ICO to investigate and, or review our data processing activities.

We will have regard to advice and guidance produced by the ICO and will endeavor to align our practices to any published codes of practice.

Further information

For further information please contact the DPO and dpo@lincolnshire.gov.uk.

Policy review

This policy will be reviewed annually.

Document control

- policy owner: Amy Jaines, information governance manager (DPO)
- published: May 2018
- last reviewed: March 2025
- version number: V3.0
- change history:
  - May 2018 - V1.0 published
  - March 2019 - V1.0 annual review, no significant change
  - March 2020 - V1.0 annual review, no significant change
  - March 2021 - V2.0, annual review, updated to reflect legislative changes brought by the UK's withdrawal from the EU

- March 2022 - V2.0, annual review, no significant change
- March 2023 - V2.0, annual review, no significant change
- March 2024 - V2.0, annual review, no significant change
- March 2025 - V3.0, annual review, full policy re-writes to present content in more accessible and plain language, reducing the use of technical terminology
- October 2025 - V3.1 amended timescale for responding to data protection related complaints from 15 working days to one calendar month