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 aims to outline our commitment and approach to achieving our obligations as required by data protection legislation.

Scope

This policy applies to:

- all personal data that we process regardless of its format
- any individual processing personal data that we hold

Definitions

The following definitions shall apply:

Data Protection Legislation means:

- The UK General Data Protection Regulation ("UK GDPR")
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations 2003 (as amended), and
- Any other applicable law concerning the processing of personal data and privacy

Data means information which:

- is processed wholly or partly by automated means
- is processed other than by automated means and forms part of a filing system. For example a structured set of data which are accessible by specific criteria
- is processed other than by automated means and is intended to form part of a filing system

Personal data means any information, which either directly or indirectly, relates to an identified or identifiable living individual. 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 means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature
- whether a person is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- biometric and, or genetic data
- sex life or sexual orientation

Criminal Convictions Data means 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 in relation to information or data, means any operation(s) performed on personal data or sets or personal data (whether automated or not) such as:

- collection
- use
- Storage
- disclosure
- dissemination
- destruction

Data subject means an individual who is the subject of personal data.

Controller means a person or organisation who (either alone or jointly with others) determines the purpose and means of processing.

Processor, in relation to personal data, means any person or organisation (other than an employee of the controller) that processes data on behalf of the controller.

Law Enforcement Processing means processing for the purpose of:

- the prevention, investigation, detection or prosecution of criminal offences, or
- the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The Six Data Protection Principles

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

- Principle 1: Personal data shall be processed fairly and lawfully and in a transparent manner.
- Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes shall not be processed in a manner incompatible with that purpose.
- Principle 3: Personal data shall be adequate, relevant and limited to what is necessary for the purpose.
- Principle 4: Personal data shall be accurate and, where necessary kept up to date.
- Principle 5: Personal data shall be kept in a form that permits identification for no longer than necessary.
- Principle 6: Personal data shall be processed in a manner that ensures appropriate security.
- In addition, we shall ensure that we comply with the 'accountability principle'. This requires us to have appropriate processes and records in place to demonstrate our compliance with the principles listed above.

Our responsibilities

We shall ensure that:

- we pay the annual statutory data protection fee to the Information Commissioner's Office. Our data protection registration number is Z8397628
- we have in place appropriate policies and processes which aim to support us to meet our obligations under data protection legislation
- we have specialist staff with specific responsibility for providing support and guidance
- staff processing personal data understand that they are responsible for complying with the data protection principles and are appropriately trained

Data Protection Officer (DPO)

We will have in place a DPO. They are responsible for supporting 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 all data subjects
- act as the single point of contact for the Information Commissioner's Office and any other bodies engaged in the application of data protection legislation

Data Protection roles and responsibilities

In addition to the DPO the following roles are established:

The Senior Information Risk Owner (SIRO) is the owner of information risk management at director level. They are responsible for leading and fostering a culture that values, protects and uses information in a manner which benefits us and our service users.

Caldicott Guardians are individual senior managers within social care and public health. They ensure that our health and social care services satisfy data protection requirements and the Caldicott principles.

The Head of Information Assurance is responsible for the information assurance strategy. They assist in the identification, management and implementation of information risk.

The Information Governance Manager (and Officer role) is responsible for:

- providing information governance support, guidance, and training to staff
- ensuring that staff are aware or their data protection responsibilities and obligations

Information Asset Owners (IAO) are individuals appointed to ensure that we handle and manage specific information assets appropriately. IAO's are key decision makers across information they own.

All managers are responsible for ensuring:

- that the requirements of this policy are integrated into service procedures
- that staff comply with all relevant policies in their area of responsibility

All staff are responsible for ensuring they process information in line with this policy. This includes complying with related policy requirements and undertaking mandatory annual information assurance training.

Record of processing activity

We shall maintain a written record of our data processing activities.

The Information Assurance team shall be responsible for creating and maintaining the record of processing activity in conjunction with IAOs.

Appropriate policy documents

We shall have in place appropriate policy documents setting out our procedures for securing compliance with data protection legislation in relation to:

- processing of Special Category Data and Criminal Convictions Data; and
- Law Enforcement Processing

Privacy notices

To support open and transparent data processing we shall ensure that we make privacy notices available to data subjects.

Privacy notices will be clear, concise, and in plain English.

We will provide a copy of any privacy notice on request and free of charge.

Data Protection Impact Assessment (DPIA)

Any processing activity that is identified as involving high risk processing shall be subject to a DPIA. Such activities include:

- processing special category or criminal offence data on a large scale
- systematic monitoring of publicly accessible places
- systematic or extensive profiling

The DPIA shall be used to identify and remediate privacy risks.

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

The DPO shall be consulted on all DPIAs.

Data security

We shall ensure we have an information security management system in place that aims to reduce the risk of personal data breaches.

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

We shall 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.

Contracted services

Contracts shall include measures to ensure third parties handle personal data in accordance with data protection legislation when delivering services on our behalf.

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

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

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

We shall ensure that documented sharing agreements exist between us and partnership agencies where required.

The Information Assurance Team shall 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

The NHS has implemented a national data opt-out service. This allows individuals to choose if they do not want their data to be used for purposes beyond their individual care or treatment, specifically for research and planning purposes. All health and care organisations in England must comply.

We shall 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

We shall have processes in place for considering requests for the disclosure of data that falls within the scope of the national data opt-out.

Individual rights

We shall ensure that adequate processes are in place to support individuals who wish to exercise their rights in respect of their personal data.

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

We shall refer complaints regarding how we process personal data to:

- the relevant service area in the first instance
- to the council's Customer Relations Team if the matter cannot be resolved

Training and awareness

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

Individuals shall maintain a good awareness of data protection.

Additional training shall be provided where appropriate.

Surveillance camera systems

Images and audio recordings of identifiable individuals captured by surveillance camera systems amount to personal data relating to that individual. They will be subject to the same provisions and safeguards afforded by data protection legislation as other types of recorded information.

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 shall not transfer personal data outside the United Kingdom, unless:

- there is a legal requirement to do so or
- it can be evidenced that appropriate safeguards are in place as required by data protection legislation

Information Commissioner's Office

We shall comply fully with all requests from the Information Commissioner's Office to investigate and, or review our data processing activities.

We shall have regard to advice and guidance produced by the Information Commissioner's Office as far as it relates to our data processing activities.

We shall consider any code of practice published by the Information Commissioner's office and shall endeavour to align our practices accordingly.

Further information and review

For further information please contact the DPO and dpo@lincolnshire.gov.uk or the Information Assurance Team at IA@lincolnshire.gov.uk

Policy review

We shall review this policy on an annual basis.