Greater Lincolnshire
Combined County Authority

Policy

Data Protection

Purpose

Greater Lincolnshire Combined County Authority has a statutory duty to meet obligations, as set out within data protection legislation, as we process personal data when conducting our business.

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

Document Owner	S73 Officer
Document Version	V1.1
Approved By	GLCCA 29 April 2025
Date of Next Review	

Contents

Scope

This policy applies to:

- All personal data, regardless of format, processed by us.
- Any individual processing personal data held by us.

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 and any other applicable law concerning the processing of personal data.

Data means information which:

- Is processed wholly or partly by automated means,
- Is not processed by automated means and forms part of a relevant filing system i.e. a structured set of data which are accessible by specific criteria,
- Is not processed 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 individual. Identifiers include name, address, date of birth, unique identification numbers (such a pupil reference numbers), location data, online identifiers (such as IP addresses), pseudonymised data and information relating to a person's social or economic status.

Data subject means the person who can be identified from the information.

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,
- Affiliation with a trade union,
- Physical or mental health or condition,
- Biometric and/or genetic data
- Sex life or sexual orientation.

Criminal Convictions Data means personal data concerning:

- The commission or alleged commission of any offence, or
- Any proceedings resulting from any offence or alleged offence committed and the resulting action

Processing in relation to information or data, means any operation(s) performed on personal data (whether automated or not) such as collection, use, storage, distribution and destruction.

Controller means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed. For the purpose of this policy, the GLCCA is a Controller.

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

The 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 and 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 not be kept in a form that permits identification for longer than is necessary.

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

We shall ensure that we also comply with the 'accountability principle' which requires that we 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 data protection fee to the Information Commissioner's Office.
- We have staff in post with specific responsibility for ensuring compliance with data protection legislation.
- Staff processing personal data understand that they are responsible for complying with the data protection principles and that processing activities meet a lawful basis for processing (see Appendix A).
- Staff processing data are appropriately trained to do so.
- Staff are provided with appropriate data protection training, support and guidance.

Data Protection Roles and Responsibilities

The following roles are in place to help us achieve compliance with data protection legislation:

- The **Monitoring Officer** has overall responsibility for ensuring we operate in a manner compliant with data protection legislation and for ensuring compliance with this policy.

- The **Senior Leadership Team** have responsibility for supporting the Monitoring Officer and Data Protection Officer by ensuring individuals are aware of, and apply, this policy.

- The **Data Protection Officer (DPO)** will support us in meeting our obligations under data protection legislation by monitoring ongoing compliance, providing advice and assistance on all data protection matters as well as acting as a single point of contact for data protection queries from data subjects and the Information Commissioner's Office.

- All **Staff** have a responsibility to meet the requirements of this policy. This includes complying with individual policy requirements and undertaking training relevant to their role.

Record of Processing Activity

We shall maintain a record of its processing activities. The DPO shall be responsible for creating and maintaining the record of processing activity in conjunction with the Monitoring Officer.

Privacy Notices

We shall ensure that appropriate privacy information is made available to any data subject whose data is processed by us.

Privacy notices will explain in general terms:

- The purpose for which we will process the data collected;
- Why the data is held and for how long;
- Where we get personal data from and with whom it is shared with; and
- Contact details of relevant staff to allow requests for further information.

Privacy notices shall be published on the website and, upon request, shall be provided in hard copy, free of charge.

Data Protection Impact Assessment (DPIA)

We shall complete a DPIA at the early stages of any new processing activity where it is identified that high risk processing is present e.g. large-scale processing, processing special category data or introducing systematic monitoring.

The DPO shall be consulted on all DPIAs.

Data security

We shall ensure we have adequate technical and organisational controls in place which aim to reduce the risk of theft, loss or unlawful processing of personal data.

Security policies and procedures shall be made available to all staff.

We shall record and investigate all personal data breaches.

Where it is determined that a personal data breach results in a risk to the rights and freedoms of an individual(s) we shall 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.

Contracts and Information Sharing

Contracts with suppliers that deliver services on our behalf, and which involve the processing of personal data, shall include measures to ensure personal data is handled in accordance with data protection legislation.

We shall ensure that whenever personal data is shared with a third party, it is justified and necessary to meet a lawful basis for processing as set out in Appendix A to this policy.

Where necessary, we shall ensure that information sharing agreements exist between ourselves and partner organisations.

We shall ensure that before personal data is shared with any third party, as required by a contract or otherwise, appropriate security controls are in place.

Individual Rights

We shall ensure that adequate processes are in place to support individuals to exercise their rights in respect of their personal data (subject to exemptions) and that those processes are clearly communicated to individuals whose data is being processed.

We shall consider complaints regarding how we process personal data. Complaints shall be referred to the Complaints procedure in the first instance.

Individuals shall be made aware of their right to make a complaint to the Information Commissioner's Office and their ability to seek judicial redress.

Training and Awareness

We shall provide mandatory annual data protection training to all staff handling personal data. Additional training shall be provided where appropriate.

All staff shall maintain a good awareness of data protection and the requirements of this policy.

International Transfers

We shall not transfer personal data outside of 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.

Any systematic sharing of personal data outside of the UK shall be subject to a DPIA.

Information Commissioner's Office

We shall comply fully with all requests from the Information Commissioner's Office to investigate and/or review it’s 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 take into account any code of practice published by the Information Commissioner's Office and shall endeavour to align its own practices accordingly.

Further Information

For further information regarding data protection please contact:

DPO@greaterlincolnshire-cca.gov.uk

Data Protection Officer (GLCCA),
Lincolnshire County Council,
County Offices,
Newland,
Lincoln,
LN1 1YL

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

Review

This policy shall be reviewed annually.

Appendix A – Lawful Bases for Processing

In all processing activities, you must have a valid lawful basis in order to process personal data. You must determine the lawful basis before you begin processing and this must be appropriately documented. No single basis is 'better' or more important than the others – which basis is most appropriate will depend on the purpose for processing and our relationship with the individuals concerned.

There are six available lawful bases for processing personal data:

1. **Consent** – freely given, informed and evidenced by a clear affirmative action.
2. **Contract** – necessary for the performance of a contract with the Data Subject (including specific steps before entering into a contract).
3. **Legal Obligation** – necessary to comply with the law.
4. **Vital Interests** – necessary to protect the life of the data subject.
5. **Public Task** – necessary to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
6. **Legitimate Interests** – necessary for our, or a third parties, legitimate interests in circumstances where the Data Subject's right to privacy does not override those legitimate interests (NB. This legal basis is unavailable for public authorities when the processing is in connection with an official task).

If you are processing Special Category Data, you must also identify a further lawful basis. There are ten available lawful bases for processing Special Category Data:

1. **Explicit Consent** – freely given, informed and evidenced by a clear affirmative statement.
2. **Employment, social security or social protection law** – necessary to meet legal obligations in these specific areas.
3. **Vital Interests** – necessary to protect the life of the data subject or another individual where they are physically or legally incapable of giving consent.
4. **Not-for-profit Bodies** – processing carried out by a political, philosophical, religious or trade union.
5. **Deliberately made public by the Data Subject** – data that has manifestly been placed in the public domain by the Data Subject.
6. **Legal Claims** – for establishing, exercising or defending legal rights.
7. **Substantial Public Interest** – necessary for reasons of substantial public interest e.g. official functions, statutory purposes, equal opportunities or preventing or detecting unlawful acts.
8. **Health and Social Care** – necessary to preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, provision of health or social care or treatment or management of health and social care systems.
9. **Public interest in the area of Public Health** – such as threats to health or ensuring high standards of healthcare.
10. **Archiving Purposes** – public interest, scientific and historical research purposes or statistical purposes.

Further lawful bases are available for processing Criminal Convictions Data and advice must be sought prior to processing to determine what the appropriate lawful basis is.