
LINCOLNSHIRE COUNTY COUNCIL

Information Assurance

Data Protection Policy

V 3.4

Document Control

Reference	Data Protection Policy V 3.4
Date	5 June 2019
Author	Amy Jaines, Data Protection Officer
Approved by	Andrew Crookham, Senior Information Risk Owner

Version History

Date	Version Number	Revision Notes	Author
5 March 2014	V 2	Document structure changed. Removed procedure and guidance. Removed references to schools. Updated definitions to reflect ICO definitions. Updated DPA principles. Amended information sharing/contracts/data subjects.	David Ingham
20 March 2014	V 2.1	Minor amendments following comments from Legal Services inc: Clarification of a relevant filing system provided. Clarification of an accessible record provided.	David Ingham
22 May 2014	V 2.2	Minor amendments following CIO comments. Published.	David Ingham
22 June 2015	V 2.3	Document review, minor amendments. Published	David Ingham
30 June 2016	V 2.4	Word Issue and next review date to publish added to document control section and policy review statement included	Sally Ward
30 June 2016	V 2.5	Document review, no amendments.	Sally Ward
15 June 2017	V 2.6	Document review, minor amendments.	Kathryn Irwin-Banks
20 July 2017	V 2.7	Minor amendments. SIRO change.	Kathryn Irwin-Banks
09 March 2018	V 3.0	Amended and restructured to reflect new legislative requirements contained within GDPR and the Data Protection Act [2018] (subject to Royal Assent)	Amy Jaines
10 April 2018	V 3.1	Amended 'Information Sharing' and added Appendix A – Lawful Bases for Processing	Amy Jaines
03 July 2018	V3.2	Updated to reflect the confirmed implementation of the Data Protection Act 2018	Amy Jaines
01 February 2019	V3.3	Document review, minor amendments, update SIRO details	Amy Jaines
05 June 2019	V3.4	Amendments to Section 17 – CCTV, update SIRO details	Amy Jaines

Contents

Document Control	2
1. Introduction.....	4
2. Aim	4
3. Scope	4
4. Definitions.....	4
5. The Six Data Protection Principles	5
6. Council Responsibilities.....	6
7. Data Protection Officer (DPO).....	6
8. Data Protection Roles and Responsibilities	6
9. Record of Processing Activity.....	7
10. Privacy Notices.....	7
11. Data Protection Impact Assessment (DPIA).....	8
12. Data Security	8
13. Contracts	8
14. Information Sharing	8
15. Individual Rights	9
16. Training & Awareness	9
17. Surveillance Camera Systems	9
18. International Transfers.....	9
19. Information Commissioner's Office.....	10
20. Policy Review	10
Appendix A – Lawful Bases for Processing	11

1. Introduction

Lincolnshire County Council (the council) has a statutory duty to meet its obligations as set out within data protection legislation as it processes personal data when conducting its business.

2. Aim

- 2.1. The aim of the policy is to outline the council's commitment and approach to achieving its obligations as required by data protection legislation.

3. Scope

- 3.1. This policy applies to:

- 3.1.1. All personal data processed by the council regardless of its format.
- 3.1.2. Any individual processing personal data held by the council.

4. Definitions

- 4.1. The following definitions shall apply:

- 4.2. **Data Protection Legislation** means:

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

- 4.3. **Data** means information which:

- 4.3.1. Is being processed wholly or partly by automated means.
- 4.3.2. Is processed other than by automated means and forms part of a filing system i.e. structured set of data which are accessible by specific criteria.
- 4.3.3. Is processed other than by automated means and is intended to form part of a filing system.

- 4.4. **Personal data** means any information, which either directly or indirectly, relates to an identified or identifiable living individual. Identifiers include name, address, and date of birth, postcodes, unique identification numbers, location data, online identifiers (such as an IP address), pseudonymised data and information relating to a person's social or economic status.

- 4.5. **Special Category Data** means personal data consisting of information as to:

- 4.5.1. The racial or ethnic origin of the data subject.
 - 4.5.2. Political opinions.
 - 4.5.3. Religious beliefs or other beliefs of a similar nature.
 - 4.5.4. Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
 - 4.5.5. Physical or mental health or condition.
 - 4.5.6. Biometric and/or genetic data.
 - 4.5.7. Sex life or sexual orientation.
- 4.6. **Criminal Convictions Data** means personal data consisting of information as to:
- 4.6.1. The commission or alleged commission by him/her of any offence, or
 - 4.6.2. Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
- 4.7. **Processing** in relation to information or data, means any operation(s) performed on personal data or sets of personal data (whether automated or not) such as collection, use, storage, disclosure, dissemination and destruction.
- 4.8. **Data subject** means an individual who is the subject of personal data.
- 4.9. **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. A controller may also act jointly with another organisation to process personal data.
- 4.10. **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.

5. The Six Data Protection Principles

- 5.1. The council shall adhere to the six principles of data protection, which are:
- 5.1.1. Principle 1: Personal data shall be processed fairly and lawfully and in a transparent manner.
 - 5.1.2. Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes shall not be processed in a manner incompatible with that purpose.
 - 5.1.3. Principle 3: Personal data shall be adequate, relevant and limited to what is necessary for the purpose.

- 5.1.4. Principle 4: Personal data shall be accurate and, where necessary kept up to date.
 - 5.1.5. Principle 5: Personal data shall be kept in a form that permits identification for no longer than necessary.
 - 5.1.6. Principle 6: Personal data shall be processed in a manner that ensures appropriate security.
- 5.2. In addition, the council shall ensure that it complies with the 'accountability principle' which requires that the council has appropriate processes and records in place to demonstrate its compliance with the principles listed above.

6. Council Responsibilities

- 6.1. The council shall ensure that:
- 6.1.1. It pays the annual statutory data protection fee to the Information Commissioner's Office. The council's data protection registration number is **Z8397628**.
 - 6.1.2. It has in place appropriate policies and processes which aim to support the council in meeting its obligations under data protection legislation.
 - 6.1.3. It has specialist staff with specific responsibility for providing support and guidance to the council.
 - 6.1.4. Staff processing personal data understand that they are responsible for complying with the data protection principles and are appropriately trained.

7. Data Protection Officer (DPO)

- 7.1. The council will have in place a DPO responsible for supporting the council in meeting its obligations under data protection legislation.
- 7.2. The role, which is a statutory requirement, will:
- 7.2.1. Monitor the council's ongoing compliance.
 - 7.2.2. Provide advice and guidance on all data protection matters.
 - 7.2.3. Act as a point of contact for all data subjects.
 - 7.2.4. 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.

8. Data Protection Roles and Responsibilities

- 8.1. In addition to the DPO the following roles are established:

- 8.2. The **Senior Information Risk Owner (SIRO)** is the owner of information risk management at director level and is responsible for leading and fostering a culture that values, protects and uses information in a manner which benefits the council and its service users.
- 8.3. **Caldicott Guardians** are individual Senior Managers within social care and public health. They ensure that the council's health and social care services satisfy data protection requirements and the Caldicott principles.
- 8.4. The **Head of Information Assurance** is responsible for the information assurance strategy and assists in the identification, management and implementation of information risk.
- 8.5. The **Information Governance Manager (and Officer role)** is responsible for providing Information Governance support, guidance, and training to the council and ensuring that staff are aware of their data protection responsibilities and obligations.
- 8.6. **Information Asset Owners (IAO)** are individuals appointed to ensure that specific information assets are handled and managed appropriately. IAO's are key decision makers across information they own.
- 8.7. All **LCC Managers** are responsible for ensuring that the requirements of this policy are integrated into service procedures and that staff comply with all relevant policies in their area of responsibility.
- 8.8. All **Council Staff** are responsible for ensuring they process information in line with this policy. This includes complying with related policy requirements and undertaking mandatory annual IG training.

9. Record of Processing Activity

- 9.1. The council shall maintain a written record of its data processing activities.
- 9.2. The Information Assurance team shall be responsible for creating and maintaining the record of processing activity in conjunction with Information Asset Owners.

10. Privacy Notices

- 10.1. To support open and transparent data processing the council shall ensure that privacy notices are made available to data subjects.
- 10.2. The council will adopt a layered approach to privacy notices i.e. Corporate/Directorate/Function (where necessary).
- 10.3. Privacy notices will be clear, concise, and in plain English.
- 10.4. A copy of any privacy notice shall be provided on request and free of charge.

11. Data Protection Impact Assessment (DPIA)

- 11.1. The council shall aim to complete a DPIA at the early stages of any processing activity that involves high risk processing. Such activities include processing on a large scale; systematic monitoring; or processing special category data.
- 11.2. The DPIA shall be used to identify and remediate privacy risks.
- 11.3. Staff shall consult with the Information Assurance team at an early stage to identify DPIA requirements.
- 11.4. The DPO shall be consulted on all DPIAs.

12. Data Security

- 12.1. The council shall ensure it has an information security management system in place that aims to reduce the risk of personal data breaches.
- 12.2. Security policies and procedures shall be made available to all staff.
- 12.3. The council shall record and investigate all personal data breaches.
- 12.4. Where it is determined that a breach results in a risk to the rights and freedoms of an individual(s) the council will aim to report the breach to the Information Commissioner's Office within 72 hours of becoming aware.
- 12.5. Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) the council shall inform the individual(s) without undue delay.

13. Contracts

- 13.1. Contracts shall include measures to ensure personal data is handled in accordance with data protection legislation.
- 13.2. Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be used or disclosed for any other reason.
- 13.3. The council shall ensure that before personal data is shared with a third party as part of a contract, appropriate security controls are in place.

14. Information Sharing

- 14.1. The council shall ensure that information is shared only when it is within the provisions of data protection legislation.
- 14.2. The council shall ensure that when information is shared it is justified and necessary to meet a lawful basis for processing as set out at Appendix A to this policy.
- 14.3. The council shall ensure that adequate security is in place to protect the data when it is shared with another organisation and that information sharing arrangements are documented.

14.4. The council shall ensure that information sharing agreements exist between the council and partnership agencies where required.

14.5. The Information Assurance Team shall provide the council with guidance on information sharing in the context of systematic sharing and sharing in ad-hoc, one off circumstances.

15. Individual Rights

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

15.2. The council shall respond to any request to exercise individual rights within one calendar month.

15.3. Complaints regarding how the council processes personal data shall be referred to the relevant service area in the first instance and then to the council's Customer Relations Team if the matter cannot be resolved.

16. Training & Awareness

16.1. The council shall provide mandatory annual data protection training to all staff handling personal data.

16.2. Individuals shall maintain a good awareness of data protection.

16.3. Additional training shall be provided where appropriate.

17. Surveillance Camera Systems

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

17.2. A Surveillance Camera System Policy and supporting guidance shall be made available to all staff setting out the council's commitment to meet its data protection and wider legal obligations when using such a system.

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

18. International Transfers

18.1. The council shall not transfer personal data outside the European Union, to third countries or international organisations 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.

18.2. Where it is identified that an international transfer of personal data is necessary, the council shall seek appropriate legal advice.

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

19. Information Commissioner's Office

19.1. The council shall comply fully with all requests from the Information Commissioner's Office to investigate and/or review the council's data processing activities.

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

19.3. The council shall take into account any code of practice published by the Information Commissioner's office and shall endeavour to align its own practices accordingly.

20. Policy Review

20.1. This policy shall be reviewed on an annual basis.

Appendix A – Lawful Bases for Processing

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 the council's relationship with the individual(s) 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 (inc. 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 the council's official functions, and the task or function has a clear basis in law.
6. **Legitimate Interests** – necessary for the council's, 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 Personal 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 action
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** – necessary 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.