Leicestershire County Council

Data Protection Policy

Version: 2.0

Agreed by: I&T Board

Date: May 2018

Review Date: May 2019

Document Control

Control Details

Document Location:	X:\Information and Technology\Policies and Procedures\Approved\Data Protection Policy\Products\Final
Production Software	Microsoft Word
Author:	Information Governance Team
Owner:	Information Governance Team

Document Amendment Record

Issue	Amendment Detail	Author	Date
0.1	First Draft	KM	09 Aug 16
0.2	Second Draft	KM	26 Sept 16
0.3	Final Draft	KM	17 Oct 16
1.1	Transferred to new policy template	AP	02 Feb 18
2.0	GDPR published version	TB	10 Apr 18

1. Introduction

The purpose of this policy is to ensure that Leicestershire County Council and individuals working for, or on its behalf, are aware of their obligations under, and comply with, UK Data Protection Law.

Leicestershire County Council collects and processes different types of information about the people with whom it deals and communicates with in order to provide its services to the community.

It is the Council's obligation, as the Data Controller, to ensure compliance with UK Data Protection Law.

The following policy outlines the Council's responsibilities and processes surrounding the personal data which is processed by the Council and its employees.

2. Scope

This policy applies to:

- All forms of information and data owned, administered, stored, archived or controlled by the Council, including electronic and hard copy formats,
- Information and data in test, training and live environments, however it is hosted.
- All elected members and staff of the Council including temporary and contract staff, volunteers and third-parties accessing or using the Council's information, data and/or network; and
- All electronic and communication devices owned, administered, controlled or sanctioned for use by the Council.
- All Service users and members of the public whose personal information is held by the Council in order to provide its services.

3. Policy Statement

The Council has to collect and use personal and/or sensitive information about people in order to operate. This includes information about;

- Members of the public, service users, clients and customers.
- Current, past and prospective employees.
- Suppliers and other third parties.

In addition, the authority may have to collect and use information in order to comply with the legal requirements of central government. This personal information must also be handled in line with the law.

Therefore the Council is committed to:

- complying with both law and good practice.
- respecting individuals' rights.
- being open and honest with individuals whose data is collected and held.
- providing training and support for staff who handle personal data, so that they can act confidently and consistently.
- ensure retention and disposal of personal information is adhered to.
- Implement appropriate technical and organisational security measures to safeguard personal information are in place.
- ensure personal information is not transferred abroad without suitable safeguards or adequate protection.
- ensure the quality of information used by the Council.

To this end the Council will only process personal or special category data where an appropriate legal basis can be identified.

The lawful bases for processing are set out in Article 6 of the General Data Protection Regulations (GDPR). At least one of these must apply whenever the Council is processing personal data:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If the Council is processing special category data then both an article 6 and article 9 conditions are required. The article 9 conditions are detailed below:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. processing is 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 and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which

provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Further conditions are available within the Data Protection Bill. For help and advice in determining the appropriate condition contact the Information Governance Team.

Where the Council is processing personal data it fully endorses and follows the principles of GDPR outlined below.

Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency');

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation');

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy');

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation');

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality').

Furthermore the Council is responsible for, and must be able to demonstrate compliance with the 6 principles above (‘accountability').

4. Duties and Responsibilities

Leicestershire County Council is registered as a Data Controller and responsibility for the fair and lawful processing of personal and/or sensitive personal information rests with the Chief Executive on behalf of Council as a whole.

However it is the responsibility of all employees and elected members to handle information and data correctly. As an individual representing, working for, or on behalf of, the Council it is essential that you understand and abide by the following:

- Corporate and/or departmental policy, procedures and guidance on the collection and use of personal/sensitive information and data;
- Only process personal/sensitive personal information in accordance with the Act;
- Be clear why you are using personal/sensitive information;
- Tell people why their information is being collected, what it will be used for and how it will be managed from collection to destruction;
- Collect only the minimum amount of personal/sensitive data needed, and use it only for the purposes specified or in line with legal requirements;
- Only access the personal/sensitive data that you require to carry out your role and no more;
- Ensure the personal/sensitive information is input correctly and accurately
- Ensure personal/sensitive information is destroyed securely when it is no longer required;
- If you receive a request from an individual for information held by the Council about them please refer to the advice on intranet.
- Handle all personal information in accordance with the Council's security policies and procedures;
- Don't send personal/sensitive personal information outside of the UK without referring to the Information Governance Team.
- Understand and undertake the mandatory training relating to Information Security and Data Protection in a timely manner.

The Council will ensure that;

- Employee and Member training needs are identified and training provided to ensure that those managing and handling personal/sensitive information understand their responsibilities and follow good practice.
- Anyone who makes a request regarding their personal information to the Council is responded to.

5. Data Subjects Rights

The GDPR outlines several data subject rights and the Council will ensure that the rights of people about whom information is held can be fully exercised. The rights are as follows:

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

Further details surrounding this right can be found in the Data Capture and Storage Policy.

The right of access (also known as Subject Access Requests)

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information — this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

This Council must provide a copy of the information free of charge. However, a ‘reasonable fee' can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt.

This can be extended by a further two months where requests are complex or numerous. If this is the case, the Council must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Council can:

- charge a reasonable fee taking into account the administrative costs of providing the information;

- or refuse to respond.

Where the Council refuses to respond to a request, it must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. The Council must verify the identity of the person making the request, using ‘reasonable means'.

If the request is made electronically, the Council should provide the information in a commonly used electronic format.

If you receive a subject access request please contact sar@leics.gov.uk. Further details of the SAR process can be found on the intranet.

The right to rectification

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification verbally or in writing.

The Council has one calendar month to respond to a request.

In certain circumstances you can refuse a request for rectification.

Contact the Information Governance Team should you receive a request of this nature.

The right to erasure

Individuals have a right to have personal data erased.

The right to erasure is also known as 'the right to be forgotten'.

Individuals can make a request for erasure verbally or in writing.

You have one month to respond to a request.

The right is not absolute and only applies in certain circumstances.

Contact the Information Governance Team should you receive a request of this nature.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data.

This is not an absolute right and only applies in certain circumstances.

When processing is restricted, the Council is permitted to store the personal data, but not use it.

An individual can make a request for restriction verbally or in writing. The Council have one calendar month to respond to a request.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Contact the Information Governance Team should you receive a request of this nature.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data

Contact the Information Governance Team should you receive a request of this nature.

The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling);
- and processing for purposes of scientific/historical research and statistics.

Objections where the Council processes personal data for the performance of a legal task or my organisation's legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation".

The Council must stop processing the personal data unless:

> it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
>
> or the processing is for the establishment, exercise or defence of legal claims.

The Council will inform individuals of their right to object "at the point of first communication" and in its Fair Processing Notice.

Objections where the Council processes personal data for direct marketing purposes?

The Council must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.

The Council must deal with an objection to processing for direct marketing at any time and free of charge.

The Council will inform individuals of their right to object "at the point of first communication" and in its Fair Processing Notice.

Objections where the Council processes personal data for research purposes?

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If the Council is conducting research where the processing of personal data is necessary for the performance of a public interest task, it is not required to comply with an objection to the processing.

Contact the Information Governance Team should you receive any requests outlining an objection to processing.

Rights in relation to automated decision making and profiling

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement);
- and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR applies to all automated individual decision-making and profiling.

This type of decision-making can only be done where the decision is:

- necessary for the entry into or performance of a contract;
- or authorised by Union or Member state law applicable to the controller;
- or based on the individual's explicit consent.

If the Council is conducting this type of decision making it must:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

If you wish to process information in this way then contact the Information Governance Team prior to doing so.

6. Caldicott

This Data Protection Policy should be read and adhered to alongside the Caldicott 3 review and its principles and recommendations. They provide a framework of quality standards for the management of confidential information within Health and Social Care services.

The Caldicott principles (listed below) provide a set of good practice guidelines to assist in the implementation of Data Protection and underpin appropriate information sharing. For Leicestershire County Council purposes these are particularly relevant for the Social Care departments

The Caldicott Principles are as follows;

1. Justify the purpose(s)
2. Don't use the patient identifiable information unless it is necessary
3. Use the minimum necessary patient-identifiable information.
4. Access to patient identifiable information should be on a strict need-to know basis.
5. Everyone with access to patient identifiable information should be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

7. Special category Data

There are additional requirements placed upon the data controller where the holding of "special category data" is concerned. Special category data relates to the following:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Where the Council processes any of the above categories of sensitive personal data there should be higher levels of security in place and greater restrictions on sharing and processing this data. Extra care should be given when you process sensitive personal data and more information can be found in the Council's Guide to information levels (classification) which gives sensitive personal data a level 3 classification. If any guidance is required please contact the Information Governance Team on informationgovernance@leics.gov.uk.

8. Information Sharing

Where the Council regularly shares personal information with our partners and other organisations an Information Sharing Agreement should be put in place. This agreement is signed by all partners to the sharing and agrees a set of standards and best practice surrounding Data Protection. Any Council department which shares personal information externally on a regular basis should contact the Information Governance Team for advice via informationgovernance@leics.gov.uk.

The Council is signed up to an Information Sharing Protocol, along with various other organisations in Leicester and Leicestershire. The protocol outlines the best practices surrounding the sharing of personal information and the agreed processes between partners whilst ensuring Data Protection law is adhered to.

9. Use of personal data in marketing or promotion

Leicestershire County Council complies with the Privacy of Electronic Communications Regulations (PECR).

PECR is a law in the UK which makes it unlawful to send direct marketing (or any promotional material with regards to goods and services) by electronic means without the consent of the receiver.

For further advice please contact the Information Governance Team via informationgovernance@leics.gov.uk

10. Responsibility of staff and members

All staff and elected members, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to personal data that they may handle in the course of their work.

All have a responsibility for Data Protection and are required to follow this policy.

All have a responsibility to ensure they have completed the mandatory Data Protection training on the learning pool, along with all other mandatory training under the Information Governance umbrella.

The Data Protection Policy sits in accordance with the following policies, which should be read in conjunction (all available on request). These policies contain further guidance in some areas of Data Protection.

Data Capture and Storage

The Data Capture and Storage Policy contains information about Privacy Notices. This will give you guidance along when a privacy notice is required and what it should contain.

Data Access and use

This policy sets out the rules for access to and subsequent use of information and data in safe and appropriate ways.

Retention and Disposal

This policy explains the steps to take to prevent the inappropriate disposal of records and ensure that their final disposal is in accordance with legislation, guidance or good practice.

Public Access to Data

This policy sets out how information owned, administered, or controlled by Leicestershire County Council (personal or non-personal) should be shared with, or be made available to the public (individuals or organisations).

Information Security and Acceptable Use Policy

The Information Security and Acceptable Use Policy will give you information on how to comply with Data Protection requirements for the appropriate technical and organisational measures.

11. Data Protection Governance

The following outlines the reporting arrangement around Data Protection within the Council:

- Monthly reporting to IAG around:
    - Training stats
    - SAR requests
    - Incidents (number and trends)
    - Any issues to raise to Caldicott meetings
- Quarterly reporting to departmental IT boards:

    - Training stats
    - SAR requests
    - Incidents (number and trends)
- Standing agenda items at all Caldicott guardian meetings
    - Training stats
    - SAR requests
    - Incidents (number and trends)
- 6 monthly report to CMT on IG Governance at LCC to be drafted by DPO. Will include specific items that need to be raised as well as routine updates on:
    - Training stats
    - SAR requests
    - Incidents (number and trends)

The reporting will be based around the following KPIs:

- 90% of incident reported investigated in time frame as defined in the incident process
- 90% of incidents reported within timescales defined in incident process
- 90% of actions identified from incidents completed within timeframe
- 90% of staff completed the mandatory training
- 80% of SARs answered within statutory timeframes

12. Policy Review

A review of this policy will take place at least annually or as required to take account of any new or changed legislation, regulations of business practices.

13. Breaches of this policy

Failure to adhere to this policy will place the Council at significant risk and may also result in a breach of legislation.

All breaches and suspected breaches of this policy must be reported via the intranet:

Actions or neglect leading to a breach of this policy, or failure to report a breach will be investigated.

14. Monitoring

All activity and information placed on or sent over Leicestershire County Council systems is monitored as defined by the Information Security and Acceptable Use Policy. Logs created as part of this monitoring may be used to investigate suspected unauthorised use or breach of the Information Security and Acceptable Use Policy. For third party systems these logs must also be created and made available to the Council on request.