CITY OF Lincoln COUNCIL

# Data Protection Policy

**Document control**

| | |
|---|---|
| Organisation | City of Lincoln Council |
| Title | Data Protection Policy |
| Author - name and title | Sally Brooks-Data Protection Officer |
| Owner - name and title | Sally Brooks-Data Protection Officer |
| Date | May 2018 |
| Approvals | March 2018 - Executive |
| Filename | Data Protection Policy |
| Version | V.4.0 |
| Next review date | January 2025 |

**Document Amendment history**

| Revision | Originator of change | Date of change | Change description |
|---|---|---|---|
| V.2.0 | Sally Brooks,<br>Data Protection Officer | May 2018 | To incorporate the GDPR and Data Protection Bill- following Royal Assent to be the Data Protection Act 2018. |
| V.3.0 | Sally Brooks,<br>Data Protection Officer | January 2021 | General review of policy and changes following Brexit and UK GDPR |
| V.4.0 | Sally Brooks<br>Data Protection Officer | January 2023 | General review of policy, references changed to the Data Protection Legislation. |

**Distribution and training history**

| **Details** | **Date** |
|---|---|
| Mandatory policy delivered and accepted by all staff and members | May 2018 |
| Separate annual data protection e-learning training delivered as mandatory. | Annually |
| Review and update of policy available to staff on NET-consent | March 2021 |
| Review and update of policy available to all staff and members on NET-consent. Publically available on council's website. | January 2023 |

**Contents**

## Overview

To perform efficiently the City of Lincoln Council ("the council"), must collect and use information about the individuals with whom we work. This may include members of the public, employees (past and prospective), volunteers, work experience, partner organisations, agents, customers, and suppliers. The council may also be required by law to collect and use information to meet the requirements of central government.

All personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means. We all have a responsibility for its safe handling.

This document sets out the principles of data protection; our responsibilities; the rights of individuals; information sharing; and how we shall deal with complaints. The council must comply and fully endorses the principles of data protection as set out in the Data Protection Legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), the Privacy and Electronic Communications Regulations (PECR) and any other relevant and subsequent legislation regarding the processing of personal data.

The council is a controller and is therefore bound by a legal duty to meet its obligations under the Data Protection Legislation at all times, when handling personal information. These legal obligations last from the moment the information is obtained until it is returned, deleted, or destroyed.

## 1. Purpose

The main purpose of this Policy is to raise awareness amongst staff and elected members of the Data Protection Legislation. This is to ensure that the council complies with its legal obligations at all times when handling personal information. The council also regards the lawful and correct treatment of personal information as essential to the effectiveness and success of its operations and in maintaining trust between the council and those with whom it carries out business. To this end the council will process personal information lawfully and correctly by embedding this policy into its culture, its processes, and its procedures.

## 2. Scope

### 2.1 Who does this Policy apply to?

This policy applies to all full time and part time employees of the City of Lincoln Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers and students or trainees on placement with the council.

Elected members are controllers in their own right and must ensure that any personal information they hold/use in their office as an elected member is treated in line with the Data Protection Legislation.

## 2.2 What is personal data?

This Policy applies to personal data which means

***'any information relating to an identified or identifiable natural person ('the Data Subject').***

***'an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier'***

The definition of personal data has been expanded to reflect changes in technology and includes online identifiers such as an IP address and location data where they directly or indirectly identify individuals.

Data which has been pseudonymised (key coded with reference to additional data) can also fall within the definition of personal data depending on how difficult it is to attribute the pseudonym to a particular individual.

## 2.3 What is special category data?

There are special categories of personal data also referred to as sensitive data which require extra protection. These categories are personal data revealing and concerning

- racial or ethnic origin (for example CCTV images of individuals attending a place of worship or arrangements to allow a staff member to pray)
- political opinions (not made public by the data subject)
- religious or philosophical beliefs (for example veganism or atheist)
- trade union membership
- genetic or biometric data (for example fingerprints, DNA, iris and voice/face recognition) when used for purposes of identifying an individual.
- mental or physical health (for example sickness records, occupational health reports)
- sex life
- sexual orientation (including transgender and gender reassignment)

Criminal offence data and criminal prosecutions data including investigations also require extra protection and are dealt with separately under the council's Special Category, Criminal Offence and Sensitive Law Enforcement processing policy.

## 2.4 What type of personal records does this Policy apply to?

This Policy applies to all personal data created or held by the council, in whatever format (for example paper, electronic, email, microfiche, film, photographs) and however it is stored, (for example ICT system/database, Intranet, filing structure, email, cloud, filing cabinet, shelving and personal filing drawers).

The Data Protection Legislation has expanded the scope of applicable information to include

***'the processing of personal data both automated and manual which form part of a filing system, or are attending to form part of a filing system'*.**

A filing system is where personal data is accessible according to specific criteria and this includes chronologically ordered sets of manual records containing personal data such as an officer's notebook.

The Data Protection Legislation does not apply to information about deceased individuals, although the council may owe a duty of confidentiality in relation to such information or to the use of personal data purely for personal or household activities.

## 3. Policy

### 3.1. The data protection principles

The Data Protection Legislation states that anyone processing personal data must apply the data protection principles. These principles are legally enforceable.

In summary, the principles require that personal data shall be:

1) processed fairly, lawfully and in a transparent manner; ***(lawful, fair and transparent principle)***

   *Personal data must not be processed unless at least one lawful basis has been met. Special category data requires at least one further condition to be met, in addition to the lawful basis. See the 'Definitions' section below for a list of the lawful bases and additional conditions required for processing special category data.*

2) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those processes; ***(purpose limitation principle)***

   *Further processing for archiving in the public interest, scientific or historical research or statistical purposes are not considered incompatible with initial purposes provided appropriate safeguards are in place.*

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; ***(data minimisation principle)***

4) accurate and where necessary kept up to date; ***(accuracy principle)***

   *Every step must be taken to ensure personal data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.*

5) kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed; ***(storage limitation principle)***

   *Personal data may only 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 subject to technical and organisational measures in order to safeguard the rights and freedoms of individuals.*

6) 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 principle)***

7) A further **(*accountability principle)*** requires the council as a controller to be responsible for, and be able to demonstrate, compliance with the above principles.

Accountability includes the council keeping records of all processing of personal data. These records are kept in the council's Information Asset Register and Information Asset Owner's (IAO's) are responsible for keeping their section of this up to date.

For further information, staff and members please refer to the 'IAO Handbook' available on the council's policy management software NET-consent.

These records of processing include the retention and disposal schedules for each area, which are available on the council's website at www.lincoln.gov.uk/privacy-policy

### 3.2. Responsibilities

City of Lincoln Council is a controller under the Data Protection Legislation and is subject to legal obligations regarding the protection of personal data.

The Chief Executive and the Senior Information Risk Officer (SIRO) have overall responsibility for ensuring compliance with the Data Protection Legislation within the council.

Directors, Assistant Directors, City Solicitor and s151 Officer (Finance) are responsible for ensuring compliance with the Data Protection Legislation and this Policy within their directorates.

Information Asset Owners (IAO's) are responsible for ensuring business areas they have responsibility for have processes and procedures in place that comply with the Data Protection Legislation and this Policy.

IT services are responsible for ensuring that data within systems under the control of the council, cannot be accessed by unauthorised personnel and data cannot be tampered with, lost or damaged.

Responsibility for compliance with this Policy and communicating the Policy to staff/members in their own business areas is delegated to the IAO's. IAO's have been advised of their responsibilities and the requirement to carry out ongoing risk assessments on the information assets for which they are responsible.

The responsibility for providing day-to-day advice and guidance to support the council in complying with the Data Protection Legislation and this Policy rests with the SIRO and the Data Protection Officer (DPO).

All members of staff or agency staff and elected members who hold or collect personal data are responsible for their own compliance with the Data Protection Legislation and must ensure that personal data is kept and processed in-line with the law and the Staff Code of Conduct/Members Code of Conduct.

IAO's have responsibility for agency staff's, volunteers, work experience's compliance with the law and the Staff Code of Conduct. This includes the provision of appropriate training and

inductions. IAO's must also ensure that their data protection responsibilities are communicated and handed over clearly to the successor to their IAO role.

Failure to comply by any staff/elected member may result in disciplinary action and may lead to dismissal, in addition to the possibility of an individual being criminally prosecuted under the Data Protection Legislation and/or liable to pay compensation in any civil action.

### 3.3. Engaging a processor to process personal data on behalf of the council

If a contractor, partner organisation or agent of the council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, the lead council officer must ensure a binding contract is in place.

The contract must meet the requirements of the Data Protection Legislation and due diligence is required at the procurement stage to data protection compliance particularly where personal data and special category data will be processed.

There is guidance on what needs to be included in a contract processing personal data in the IAO Handbook (see above) and in procurement policy notes issued by the Crown Commercial Service at www.gov.uk

### 3.4 Sharing personal data with other controllers

If the council is sharing personal data with other controllers such as a partner organisation, agents, or other councils then they must do so in a transparent manner. This includes determining responsibilities under the Data Protection Legislation and informing data subjects of this (privacy notices).

Information Sharing Agreements (ISA's) are required between controllers where there is systematic and regular sharing. These should be agreed and signed off before any work/sharing commences. They should record as a minimum the purpose of the sharing, the lawful basis, accuracy of data, retention of data, data necessary, security of the transfer, responsibility for privacy notices and information rights requests, any duty of confidentiality owed, security of the data, single point of contact details and review dates.

Details of ISAs in place should then be added to the corporate ISA list held in the IAO's Microsoft Teams Channel. ISA guidance and templates are also available to download from the Data Protection Page on the council's intranet Hub.

The council promotes information sharing and partnership working where it is in the best interests of the data subject. The council has an Information sharing policy and protocols in place and will keep to the standards set out in these protocols. The council as a controller must ensure, when personal data is shared, it is done in accordance with the Data Protection Legislation.

## 4. Rights of individuals

The Data Protection Legislation provides the following rights for individuals in relation to their personal data.

1. right to be informed

2. right to access
3. right to rectification
4. right to erasure (deletion)
5. right to restrict processing
6. right to data portability
7. right to object
8. rights related to automated decision making and profiling
9. rights in relation to processing based on consent (see below)

### 4.1 Right to be informed

An individual has a right to be informed of certain information concerning how their personal data will be processed. This is usually provided in a privacy notice. When and what information is supplied to the data subject depends on whether the personal data has been provided directly to the council by the data subject or via a third party. If provided directly to the council, this privacy information must be supplied to the data subject at the time their personal data is obtained. The information must be concise, transparent, intelligible, and easily accessible, as well as written in clear plain language and free of charge.

The council has a privacy notice available on its website at www.lincoln.gov.uk/privacy-policy/

This right does not apply when the data subject already has the information and in other limited circumstances where the personal data was supplied via a third party.

The Information Commissioner's Office (ICO) has produced guidance in the form of a table, which summarises the information which must be supplied in a privacy notice and which is reproduced at Appendix 1.

### 4.2 Right to access

Individuals have the right to obtain confirmation their personal data is being processed, to access their data (receive copies or self-serve) and information supplied in a privacy notice.

Requests from data subjects for copies of personal data the council holds about them are referred to as Subject Access Requests (SARs).

The council must provide free of charge a copy of any personal data held about them. However, a reasonable fee can be charged when the request is 'manifestly unfounded or excessive', particularly if repetitive. The council may also charge a fee to provide further copies of the same information. The fee must be based on the administrative cost alone of providing the information.

There is no definition of what makes a request 'manifestly unfounded or excessive'. It will depend on the particular circumstances of the request. As an example, the council may consider a request to be 'manifestly unfounded' when it is clear that it has been made with no real purpose except to cause harassment or disruption to the council. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit. A request may be considered 'excessive' if it repeats the substance of previous requests or it overlaps with other requests. However, it depends on the particular circumstances.

Where a request is manifestly unfounded or excessive particularly repetitive the council may;

- charge a reasonable fee for the administration costs of providing the information or
- refuse the request

In refusing the request the council must explain why their request has been refused and inform them of their right to complain to the ICO, at the latest within one month of the SAR being received.

The council has a SAR process, which sets out the procedures for access to personal data and complies with the Data Protection Legislation. This process is set out on the council's website at www.lincoln.gov.uk/privacy-policy/

And guidance for staff and members in the Data Protection and requests for personal data Summary Sheet.

The individual must provide proof of their identity. Information may be withheld where the council is not satisfied the person asking for information is who they say they are. In these cases, the council may refuse to provide the information until it receives all relevant requested documents.

The council must comply with the SAR within one month (28 days) of receipt. This period can be extended by a further two months where the request is complex or numerous. In this case the council would need to inform the requester of the extension within one month of the receipt of the request and explain why the extension is necessary.

The SAR does not necessarily need to be made in writing and can be made verbally although the council encourages requesters to use the council's SAR form available on the council's website (see above). If the request is made electronically the council should provide this in a commonly used electronic format.

The council should be able to provide remote access to a secure self-service system to provide individuals with direct access to their personal data. For example, the council's system for council tax and benefits available on the council's website.

Where the request is for a large amount of data the council is permitted to ask the individual to specify the information the request relates to. The ICO have confirmed in their SAR guidance that the clock is then stopped on the 1 month (28 days) statutory response time whilst the council seeks this clarification for the requester.

### 4.3 Right to rectification

Individuals have a right to have personal data rectified if inaccurate or incomplete including by the provision of a supplementary statement. If the council has disclosed the personal data to any third parties, they must inform them of the rectification where possible. The council must also inform the individual about the third parties the council have disclosed their information to.

### 4.4 Right to erasure (deletion)

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

- where the personal data is no longer required for its purpose (kept beyond its retention period)
- where the individual withdraws their consent, and this is the only legal basis for processing
- where the individual exercises their right to object to the processing and this is successful
- the personal data is being processed unlawfully (in breach of the law)
- the personal data is erased to comply with a legal obligation
- the personal data relates to a child offering information society services

The council may also refuse to respond to a request for erasure where personal data is processed for the following reasons.

- to exercise the right to freedom of expression and information (only likely to be relevant to press releases made by the council)
- to comply with a legal obligation or for the performance of a task carried out in the public interest or exercise of official authority (the council exercising its powers and duties provided the information held is still within its retention period)
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research, or statistical purposes or
- the exercise or defence of legal claims

There are additional requirements when the request relates to children's personal data particularly online services, where they may not have been aware of the risks when they consented to the processing. This reflects the emphasis on enhanced protection of children's personal data.

The council would also be required to inform third parties of the erasure, if they have disclosed the personal data to them, unless it is impossible or involves disproportionate effort.

### 4.5 Right to restrict processing

If processing is restricted following a request. The council can hold the data but not further process it. Just enough information should be retained to ensure the restriction is respected in the future.

The council would be required to comply with a request for restriction in the following circumstances.

- where the accuracy of the personal data is contested by the requester, the council would need to be able to restrict the processing until the accuracy has been verified
- where the individual has exercised their right to object to the processing (see below) and the council are considering whether its legitimate interests override those of the individual
- when the processing is unlawful, and the requester opposes erasure and requests restriction instead
- where the council no longer requires the data, but the individual requires this to establish, exercise or defend a legal claim.

The council must inform the individual if they decide to lift the restriction on processing at any time.

### 4.6 Right to data portability

This allows individuals to request transfer of their personal data from one IT environment to another in a safe and secure way without affecting its usability.

This right only applies.

- to personal data an individual has provided to the council (includes data observed from a use of a service or device)
- where the processing is based on the legal basis of the individual's consent or for the performance of a contract and
- when the processing is carried out by automated means

This right does not apply when the council are processing on the legal basis of the performance of a task in the public interest or for official functions (the council exercising its powers and duties).

The information must be provided in a structured commonly used and machine-readable form (open source file such as a CSV not PDF). If the individual requests the council may be required to transmit the data directly to another organisation, although only where this is technically feasible.

### 4.7 Right to object

Individuals have a right to object when

- processing is based on legitimate interest or the performance of a task in the public interest or exercise of any official authority (for example the council exercising its powers and duties)
- direct marketing- any marketing including promoting the aims of an organisation directed to individuals
- processing for the purposes of scientific/historical research and statistics

The council would need to stop processing the personal data unless

- it could demonstrate compelling legitimate grounds for processing which override the interest, rights, and freedoms of the individual
- the processing is for the establishment, exercise, or defence of legal claims
- the scientific/historical research use is necessary for a public task carried out for reasons of public interest

The council need to inform where applicable individuals of their right to object at the first point of communication for example in the privacy notice and when obtaining their personal data.

The council must stop processing data for direct marketing as soon as they receive an objection. There are no exemptions or grounds to refuse an objection to direct marketing.

### 4.8 Rights related to automated decision making and profiling

Individuals have the right not to be subject to a decision when

- it is based on automated processing and
- it produces a legal effect or a similarly significant effect on the individual

The council must ensure individuals are able to

- obtain human intervention
- express their point of view and
- obtain an explanation of the decision and challenge it

The right does not apply if the automated decision

- is necessary for entering into a contract
- is authorised by law with safeguards in place, for example for the purposes of fraud or tax evasion or
- is based on the explicit consent of the individual which has been obtained prior to the automated processing or
- where the decision does not have a legal or similarly significant effect on an individual

If carrying out profiling (see the 'Definitions' section below) then the council would have to ensure appropriate safeguards are in place

- to ensure processing is fair and transparent, for example provide details of the logic involved, significance and consequences (in privacy notice)
- to implement technical and organisational measure to ensure inaccuracies are corrected and minimise risks of error, for example data quality checks and reviews
- to keep personal data, secure which is proportionate to the risk to the rights and interests of the individual and prevent discriminatory effects.

Automated decisions must not concern a child or be based on special categories of personal data unless

- explicit consent is obtained from the individual or
- processing is necessary for reason of substantial public interest on the basis of a legal obligation with specific measures in place to safeguard the individual.

### 4.9. Exemptions to individual's right to access their personal data

Under the Data Protection Legislation, it is sometimes necessary to withhold certain information that has been requested by individuals in relation to their right of access. The Data Protection Officer (DPO) or the Legal Services Manager or a member of the Legal Services team can offer advice in these circumstances. Examples of exemptions to the right to access personal data which may be available are listed in the 'Definitions' section below. The ICO also have a detailed overview of the exemptions on their website www.ico.org.uk

## 5. Exemptions to the non-disclosure of personal data

Personal data must not be disclosed except in line with the Data Protection Legislation. If it appears necessary to disclose information about a third party, advice must be sought from the DPO or the Legal Services Manager and, if both are unavailable, a member of the Legal Services team. Examples of exemptions to disclosure which may be available are listed in the 'Definitions' section below. The ICO also have a detailed overview of the exemptions on their website www.ico.org.uk

## 6. Consent

The Data Protection Legislation states that where the council are relying on the lawful basis of the individual's consent alone to process their personal data this consent must be valid. To be valid consent must be

- unambiguous (clearly given)
- freely given (a genuine choice)
- demonstrable (the council are able to evidence the consent including when it was given)
- specific (not bundled up in the small print)
- informed (provided after being given all the information as to how the personal data will be processed, in the privacy notice, see 'right to be informed' below)
- explicit for special categories (in writing)
- no silence or inaction (the council should not use opt-out boxes)

The individual must make a statement or a clear affirmative action to give valid consent, for example ticking a box, entering information, or clicking on an icon.

If consent is being obtained from a child through online services and the child is under 13 years old, then parental consent is required.

Consent is rarely relied upon as a legal basis for processing by the council unless this is a genuine choice for the individual. This is due to there being a clear imbalance of power between the individual and the council. All other legal bases should be considered first.

## 7. Privacy by design and Data Protection Impact Assessments (DPIA's)

'Privacy by design' is a legal requirement for the council under the Data Protection Legislation. In summary this means implementing safeguards to ensure the protection of personal data by default and from the outset of all projects. Safeguards such as technical and organisational security measures including pseudonymisation of data and data minimisation. This requires data protection by design to be the council's default position in relation to

- decision making
- policy formulation
- project management and
- procurement

DPIA's are the most effective way for the council to comply with our data protection obligations and to meet individual's expectations of privacy. DPIA's identify and minimise privacy risks at an early stage, protecting data subject's rights, reducing costs for the council, including officer time. Effective DPIA's also reduce the risk of enforcement action by the ICO including monetary fines, legal action, and damage to the council's reputation. DPIA's are imbedded into project development, to ensure the council is dynamic, competitive, and able to demonstrate to 'privacy by design'.

DPIA's screening assessments are good practice for all projects involving the processing of personal data.

The Data Protection Legislation states DPIA's must be carried out in certain circumstances including

- high risk processing of personal data, particularly involving new technologies
- profiling with significant effects on individuals
- large scale special category/criminal data processing
- public surveillance on a large scale (for example CCTV of a publically accessible area)

The council has extensive guidance and procedures including templates for carrying out these DPIA's which are available to staff and members on the Data Protection Page of the council's intranet Hub.

## 8. International transfers

The Data Protection Legislation requires where personal data is transferred to a third country (outside the UK), those countries need to have been judged by the ICO as adequate countries or there needs to be necessary safeguards in place. Safeguards such as a legally binding agreements between public bodies or standard contractual clauses or transfer assessments approved by the ICO. There is list of adequate countries on the ICO's website. The ICO have guidance about such transfers on their website here and advice should always be sought from the council's DPO or Legal Services before such as transfer takes place.

## 9. Further information, enquiries, and complaints

Further information and guidance on data protection is available on the ICO's website at www.ico.org.uk

Advice on the Data Protection Legislation can be sought and obtained from the Data Protection Officer (DPO) or the Legal Services Manager or a member of the Legal Services team. They are responsible for dealing with all internal and external enquires and are also the first point of contact on any of the issues mentioned in this Policy.

An individual has the right to complain about the response they have received regarding their request relating to their personal data as well as to complain about other issues concerning the handling of their data and breaches of the Data Protection Legislation. All complaints should be in writing, dated and should include details of the complainant, as well as a detailed account of the nature of the problem.

Individuals under the right to be informed must be provided with the Data Protection Officer's contact details being: Data Protection Officer, City of Lincoln Council, City Hall, Beaumont Fee, Lincoln, LN1 1DD. Telephone 01522 881188 or dpo@lincoln.gov.uk

And their right to complain to the Information Commissioner's Office: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 0303 123 113 or www.ico.org.uk

## 10. Breach of this Policy

Any breach of this Policy must be investigated in line with the Data Protection Breach Management Policy and associated procedures. The council will always treat any data breach as a serious issue and may result in a disciplinary investigation and may lead to dismissal.

The council encourages the notification of breaches of the Data Protection Legislation by staff and members at the earliest opportunity. Notification will also be considered in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach. The data breach reporting process is primarily an opportunity for lessons to be learnt and processes to be put into place or changed to avoid the breach happening again. Each incident will be investigated and judged on its individual circumstances in line with the Staff Code of Conduct/Members' Code of Conduct.

## 11. Data breach notification

The Data Protection Legislation makes it mandatory for the council to report personal data breaches defined as

***'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, transmitted, stored or otherwise processed'.***

Where the breach affects individuals' rights and freedoms the council must report this to the ICO without delay and no later than within 72 hours.

If the risk to individual's rights and freedoms is high, the council, must also report the breach, without delay, to the data subjects affected, for example the customers, partners, or staff members to which the personal data relates.

The council has its own Data Breach Management Policy and internal data breach reporting e-form system available on the Data Protection Page of the council's intranet Hub.

The decision as to whether the breach needs to be reported to the ICO or data subjects is for the Senior Information Risk Officer and the Data Protection Officer.

## 12. Policy Compliance

### 12.1. Compliance measurement

The council will ensure compliance with this Policy by regularly reviewing organisational and technological processes to ensure compliance with the Data Protection Legislation and in the provision of training for all staff and elected members processing personal data, which will be monitored and reported by Information Governance Board (Corporate Leadership Team) and Audit Committee.

All policies and procedures relating to the Data Protection Legislation and Information Governance will be subject to scrutiny by Policy Scrutiny Committee and Audit Committee.

The Data Protection Officer will keep a record of all incidents and breaches relating to the Data Protection Legislation and will deal with all correspondence with the ICO relating to data protection matters.

IAO's will be asked to declare that they are compliant in their business areas with the Data Protection Legislation by submitting an IAO Checklist to the SIRO/DPO annually and as required.

### 12.2. Non-compliance and criminal offences

A deliberate or reckless breach of the Data Protection Legislation could result in a member of staff/elected member facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this Policy and related procedures.

All personal data recorded in any format must be handled securely and appropriately, and staff/elected members must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff/elected member will be considered a disciplinary issue.

Employees should be aware that it is a criminal offence deliberately or recklessly to disclose or obtain personal data without the authority of council. It is also a criminal offence to re-identify personal data, to process this without the authority of the council and to alter, deface, block, delete, destroy, or conceal personal data to prevent its disclosure. In addition, civil actions may be brought against individuals and the council for compensation.

Non-compliance of this Policy may also result in a report being made to the ICO which could result in the council facing enforcement action, including substantial fines, in addition to substantial reputational damage.

### 12.3. Policy review

This Policy will be reviewed every two years and updated in the interim as required. Any substantial changes to be approved by Policy Scrutiny Committee and Audit Committee.

## 13. Related policies, and guidance

This Policy relates to other council policies and guidance, in particular:

Information Governance Policy
Legal Responsibilities Policy
Information Sharing Policy
Data Quality Policy
Data Protection Breach Management Policy
Freedom of Information Policy & Environmental Information Regulations Policy
Records Management Policy
Information Security Policy
Staff Code of Conduct
Member's Code of Conduct
Retention and Disposal Guidelines
Removal Guidance, Transporting data and devices
Redaction Procedures
Special Category, Criminal Offence and Sensitive Law Enforcement processing Policy.

Information Asset Owner (IAO) Handbook

Data Protection Page on Hub council's intranet for staff and elected members.

## 14. Definitions

### 14.1. Abbreviations

| Abbreviation | Description |
|---|---|
| DPA | Data Protection Act 2018 |
| EU GDPR | Regulation (EU) 2016/679 of the European Parliament and of the Council. |
| UK GDPR | From 1 January 2021, the EU GDPR was adopted into UK law by section 3 of the EU Withdrawal Act 2018 (EUWA 2018) and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (Implementing Regulations). Organisations based in the UK must comply with this version of the GDPR when processing personal data. |
| ICO | The Information Commissioner's Office |
| SIRO | Senior Information Risk Officer |
| IAO | Information Asset Owner |
| ISA | Information Sharing Agreement |
| SAR | Subject Access Request |
| DPO | Data Protection Officer |

### 14.2. Definitions

| | |
|---|---|
| The Data Protection Legislation | The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), the Privacy and Electronic Communications Regulations (PECR) and any other relevant and subsequent legislation regarding the processing of personal data. |

| | |
|---|---|
| Processing | An operation or set of operations which is performed on personal data or on sets of personal data, such as;<br>• collection, recording, organisation, structuring, storage<br>• adaptation or alteration<br>• retrieval, consultation, use<br>• disclosure by transmission, dissemination or otherwise making available<br>• alignment or combination, or<br>• restriction, erasure or destruction. |
| Controller | A person who determines the purpose for which and the manner in which, Personal Data is to be processed. This may be an individual or an organisation and the processing may be carried out jointly with other persons |
| Data subject | This is the living individual who is the subject of the Personal Data |
| Processor | A person who processes personal data on a Controller's behalf. Anyone responsible for the disposal of confidential waste is also included in this definition |
| Privacy notice | A notice the council are required to give at the time personal data is obtained from or about data subjects. The Privacy Notice must contain certain information depending on how the personal data has been received. See Appendix 1 |
| Profiling | Processing of personal data to evaluate certain aspects relating to data subjects in particular to analyse or predict behaviour, economic situation, and personal preferences. |
| Automated decision making | Decisions made solely by computers which produces a legal effect or a similarly significant effect on the individual |
| Pseudonymised data | Personal data which can no longer be attributed to a specific data subject without the use of additional information (kept separately and subject to security measures to ensure not attributed to data subject) |
| Information Commissioner's Office (ICO) | The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. www.ico.org.uk |
| Information Asset Owner (IAO) | Information Asset Owners within the council are all Service Managers and where appropriate Team Leaders. IAO's are responsible for the data held in their areas. If you are unsure of your IAO, contact the Data Protection Officer. |
| Information Asset Register | The council's Records of Processing Activities (ROPA). This records the data we hold, where it is held, who can access it, the risks to the data, security measures, who the data is shared with. Each IAO is responsible for the section of register relevant to their business area. |

| | |
|---|---|
| Legal bases for processing personal data | • necessary for a contract<br>• necessary for a legal obligation<br>• vital interests (emergency to life)<br>• necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (most relevant to the council's exercise of its powers and duties)<br>• necessary for legitimate interests (not available for the council in the performance of their public tasks)<br>• OR the data subject has given consent |
| Additional conditions for processing special category data | • necessary for legal obligations in employment law, social security and social protection law<br>• necessary to protect vital interests (emergency to life)<br>• carried out by a not-for-profit body with a political, philosophical, religious or trade union aim<br>• relates to personal data made manifestly public by the data subject<br>• necessary for the establishment, exercise, or defence of legal claims<br>• necessary for reasons of substantial public interest as permitted by law<br>• necessary for preventative or occupational medicine<br>• necessary for reasons of public interest in the area of public health<br>• necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes<br>• OR the data subject has given their explicit consent (written consent) |
| Examples of exemptions to the non-disclosure of Personal Data (reasons can be disclosed) | • Crime and Taxation<br>• National security<br>• Defence<br>• Prevention, detection, and prosecution of criminal offences<br>• Enforcement of civil matters<br>• Disclosures required by law or in connection with legal proceedings<br>• Statement made by health, education, and social care professionals |
| Examples of exemptions to the right of access (reasons not to disclose) | • Legal professional privilege (legal advice)<br>• Corporate finance- effecting markets and prices<br>• Management forecasts-redundancy<br>• Negotiations<br>• Confidential references in education training and employment. |

**Appendix 1**

| What information must be supplied in a Privacy Notice? | Data obtained directly from data subject | Data not obtained directly from data subject (for example via a third-party organisation) |
|---|---|---|
| Identity and contact details of the controller (the council) or the joint controllers (the council and others) and the data protection officer's contact details dpo@lincoln.gov.uk | ✓ | ✓ |
| Purpose of the processing and the lawful basis for the processing (see Definitions section) | ✓ | ✓ |
| The legitimate interests of the controller or third party, where applicable | ✓ | ✓ |
| Categories of personal data | | ✓ |
| Any recipient or categories of recipients of the personal data | ✓ | ✓ |
| Details of transfers to third country and safeguards, if applicable. | ✓ | ✓ |
| Retention period or criteria used to determine the retention period (see retention schedules) | ✓ | ✓ |
| The existence of each of data subject's rights | ✓ | ✓ |
| The right to withdraw consent at any time, where relevant (only where legal basis is Consent) | ✓ | ✓ |
| The right to lodge a complaint with the ICO | ✓ | ✓ |
| The source the personal data originates from and whether it came from publicly accessible sources | | ✓ |
| Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data | ✓ | |
| The existence of any automated decision making, including profiling and information about how decisions are made, the significance and the Consequences | ✓ | ✓ |
| When should information be provided? | At the time the data are obtained | Within a reasonable period (within 1 month) or at the latest, when first communication takes place: or if disclosure to another recipient, at the latest, before the data are disclosed. |