**Dundee City Council**

**Data Protection Policy 2019**

**Version Control**

|  |  |
| --- | --- |
| Document Title | **Data Protection Policy** |
| Author | Ian Smail |
| Version | 1.2 |
| Date | 2 October 2019 |
| Status | Live |

VERSION HISTORY

|  |  |  |
| --- | --- | --- |
| Version | Date Issued | Document Details/Reasons for Amendment |
|  |  | Policy update due to changes in Data Protection legislation |
|  |  |  |

DISTRIBUTION

|  |  |  |
| --- | --- | --- |
| Version | Date Distributed | Distributed To |
| 1.1 | 28/3/2019 | Kenny McKaig, Legal Services Manager for comment |
| 1.1 | 19/7/2019 | Strategic GDPR Group for comment |
| 1.2 | 30/7/2019 | Corporate Services Management Team for approval |
|  |  |  |
|  |  |  |

APPROVAL HISTORY

|  |  |  |
| --- | --- | --- |
| Version | Date Approved | Approved By |
| 1.2 | 2.10.19 | Corporate Services Management Team |
|  |  |  |
|  |  |  |

**Table of Contents**

[Policy Statement 3](#_Toc15393131)

[Scope 4](#_Toc15393132)

[Notification 4](#_Toc15393133)

[Introduction 6](#_Toc15393134)

[Definitions 7](#_Toc15393135)

[Roles and Responsibilities 10](#_Toc15393136)

[Employee Responsibility 13](#_Toc15393137)

[Provisions of the Legislation 14](#_Toc15393138)

[Lawful Bases for Processing Personal Information 15](#_Toc15393139)

[Individuals Rights 16](#_Toc15393140)

[Subject Access Requests 16](#_Toc15393141)

[Breaches 17](#_Toc15393142)

[Compliance 17](#_Toc15393143)

[Training 17](#_Toc15393144)

[Retention & Disposal of Data 18](#_Toc15393145)

[Data Sharing 18](#_Toc15393146)

[Information Security 18](#_Toc15393147)

[Related Policies/Procedures 18](#_Toc15393148)

[Issue & Review 19](#_Toc15393149)

**Policy Statement**

In order to carry out its functions as a Local Authority, Dundee City Council needs to collect and use information about people, including members of the public, current, past and prospective employees, clients and customers, and suppliers to carry out its activities.

The Council is committed to protecting the privacy and rights of all people it holds information about. It regards the fair and lawful treatment of personal information as essential to its operations and to maintaining confidence and trust between the Council and its customers. The Council will encourage and promote a culture of awareness of the General Data Protection Regulations and Data Protection 2018 and the guiding principles.

The personal information that the Council holds must be handled and dealt with appropriately, however it is collected, recorded and used. Whether the information is on paper, in computer records or recorded in any other format means there are safeguards within the legislation to ensure this.

The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business.

It is the Council’s policy to fully comply with the Data Protection legislation and all other related statutory, criminal and civil obligations to which the Council is required to adhere. This applies to the retrieval, storage, processing, retention, destruction and disposal of ‘personal information’.

**Scope**

This Policy applies to all employees and elected members as well as consultants, volunteers, contractors, agents or any other individual performing a function on behalf of the Council.

The policy is applicable to all personal data/information processed by the Council.

It is the Council’s policy to fully comply with the Data Protection legislation and all other related statutory, criminal and civil obligations to which the Council is required to adhere. This applies to the retrieval, storage, processing, retention, destruction and disposal of ‘personal information’.

**Notification**

The Council must advise the Information Commissioner's Office that it holds

personal information about living people. It must also pay a fee in accordance with

the Data Protection (Charges and Information) Regulations 2018. Dundee City Council’s registration number is Z7211936.

**Introduction**

The Council depends on computer systems and paper records to carry out its functions. The previous Data Protection Act was enacted 20 years ago during which the way and ability to share data has changed, for example access to the internet, social media and smartphones, etc.

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 updates the legislation and takes such changes into account in order to protect the rights of individuals.

**Definitions**

This section provides a description of the data protection terms used in. or relate to, the policy.

Personal Data or Information:

This is data or information which relates to a living individual (“data subject”) who can be identified:

• From the data.

• From the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

This includes the basic information such as name, address, date of birth, telephone number, national insurance number, etc. as well as any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Special Category Data(previously referred to as ‘Sensitive Data’):
This is personal data consisting of information as to any of the following:

• Racial or ethnic origin.

• Political opinions.

• Religious or philosophical beliefs.

• Trade union membership.

• Genetics.

• Biometrics (where used for ID purposes).

• Health.

• Sex life.

• Sexual orientation.

Special category personal data is subject to much stricter conditions of processing.

Record(s):

A record is recorded information, in any format, including data in systems created, received and maintained by the Council and kept as evidence of such activity.

Format:

A record can be in any format including (but not limited to) paper files, e-mail, audio/visual, electronic documents, systems data, databases, digital images and photographs.

Records Management:

The control of the Council records during their lifetime, from creation to storage until archiving or destruction.

Record Keeping System:

A system or procedure by which the records of the Council are created, captured, secured, maintained and disposed.

Processing:

The definition of processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.

Data Controller:

A Data Controller is a person or more usually an organisation that decides how any personal information can be held and processed, and for what purposes. Dundee City Council is a Data Controller. Each Councillor is a Data Controller.

Joint Data Controllers:

These are people or organisations (for example Dundee City Council, NHS Tayside or Police Scotland) who jointly process and share information based on a shared activity.

Data Processor:

This role is carried out by any person or organisation other than a Council employee (for example, contractors and agents) who process personal information on behalf of the Council.

Data Protection Impact Assessment:
An audit process to describe and analyse intended processing of personal data, helping to identify and minimise data protection risks at an early stage. Recording and reviewing the DPIA provides evidence of both considering risk and the requirement of on-going compliance.

Data Sharing Agreement:A formal document that outlines the sharing of data according to certain terms and conditions. Can be used internally, between Services, or more likely between to organisations. The document serves several purposes, those being compliance, transparency, regulation of the data to prevent misuse and that both sides understand what is expected of them

On-Going Compliance:An over-arching requirement of GDPR meaning that data controllers need to consider and evidence that they comply with the legislation.

Data protection by design and default:

A privacy-focused approach - data controllers design appropriate technical and organisational measures (a) to implement the data protection principles in an effective manner, and (b) to integrate into the processing itself the safeguards necessary for that purpose.

Privacy Notice:A requirement under GDPR, where information is made available or provided to individuals when information is collected about them summarising the activity, including why it is collected, how long it is kept and whether it is shared with anyone else.

Subject Access Request:
A request by an individual to a data controller under the Act, for any personal data processed or held by the data controller of which they are the data subject. Requests for information are usually free of charge and should be answered within one month.

Register of Processing:This Register of Data Processing sets out the Council’s activities that involve the collection and use of personal information and the reason why we can process your information lawfully.

For each activity, the Council must publish a Privacy Notice setting out how personal data is used.

**Roles and Responsibilities**

Within the Council all employees are responsible for the personal data they use and must follow any related policies and procedures. Certain Council posts are tasked with specific responsibilities in regards to data protection:

Senior Information Risk Owner (SIRO):

The Senior Information Risk Owner has overall strategic responsibility for governance in relation to data protection risks. The SIRO:

Acts as advocate for information risk at the Senior Management Team.

Provides written advice for the Annual Governance Statement relating to information risk, based on Service feedback.

Drives culture change regarding information risks in a realistic and effective manner.

Oversees the reporting and management of information incidents.

In liaison with the Chief Executive and the Executive Directors, ensures the Information Asset Owner and Information Asset Administrator roles are in place to support the SIRO role.

The Council’s SIRO is the Executive Director of Corporate Services.

Information Asset Owner (IAO):

The Information Asset Owners is the Executive Director of each Service. Their role is to understand what information is held by their service; what is added and what is removed; how information is moved or shared; who has access; how the information is used and that information about the processing is communicated. Through their Service management teams they must ensure that written procedures are in place and followed relating to these activities, risks are assessed, mitigated and the risk assessment processes are audited. IAOs will appoint Service Representatives to provide advice to members of staff.

Data Protection Officer (DPO):

The Council is required to have a named individual as the person with the overarching responsibility for ensuring compliance with the data protection and promotion of good practice throughout the organisation.

The role of the Data Protection Officer is to:

Inform and advise the Council and its employees about their obligations to comply with the General Data Protection Regulation and other data protection laws.
Monitor compliance with the General Data Protection Regulation, Data Protection Act 2018 and other protection laws, including the assignment of responsibilities, awareness raising, and training of staff involved in the processing operations and related audits.
Provide advice about data protection impact assessments and monitor their performance.
Co-operate with the supervisory authority, the Information Commissioner’s Office (ICO). Act as the contact point for the ICO on issues related to the processing of personal data.

The Information Governance Manager is the Council’s Data Protection Officer and has the overall responsibility for the administration and implementation of the Policy.

Data Protection Service Representatives:
Each Executive Director must nominate a representative to the Council’s Information Compliance and Governance Groups. The reps are responsible for providing regular advice within their Service as well as feedback on data protection around Service activities relating to the Policy and the respective Groups.

IT Services Manager:

The IT Service Manager is responsible for creating, implementing and maintaining the Council’s security policy and procedures to reflect changing local and national requirements. This includes requirements arising from legislation, security standards and national guidance. Archivist/Records Manager:

The Archivist/Records Manager will ensure that policies and procedures are compatible with legislation, particularly in relation to retention, destruction and the transfer of records to the archive and subsequent storage and access.

Information Governance Group (IGG):

The Council’s Information Governance Group, provides the strategic vision and communication with regards to the Council’s requirements in relation to implementing the Policy. The IGG is chaired by the Head of Democratic & Legal Services.

Information Compliance Group (ICG):

The Council’s Information Compliance Group, assists Services to implement good information management practices, among other functions. The ICG is chaired by the Information Governance Manager/Archivist/Records Manager.

Elected Members:

Elected Members have no automatic rights to access personal information, except, for example, when acting as a member of a committee or acting on behalf of an individual (a constituent within their ward) or under their instruction. The requirement for access must be clearly demonstrated at all times.

Elected members are bound by the terms of the legislation for the duration of their tenure of office. Elected members must, when their term of office expires or for some other reason they cease to be an elected member, arrange for the transfer or secure disposal of all personal information held by them or their support staff on their behalf.

Elected members are required to notify the Information Commissioner that they are data controllers as they hold information received from their constituents. The Council will assist with this process and pay the associated fee where required.

**Employee Responsibility:**

Training & Awareness:

Each individual who deals with personal data has a responsibility to follow the procedures and guidelines set down by the Council in relation to data protection to ensure that data is held securely; not disclosed to any unauthorised parties; to only access records for Council business and that information is disposed of securely once it is no longer required or when the retention period ends.

All relevant individuals will undertake data protection training as part of their induction and will be required to do refresher training at least every 2 years.

Further Training:
Where relevant employees have identified additional data protection responsibilities, in relation to their role, such as DPIAs for project leaders, overall responsibility for Information Asset Owners, etc. there is the requirement for further, recurring, training.

Data Protection Policy:

As with all major policies, Dundee City Council employees are required to have signed off as having read and understood the policy on an annual basis.

Information Asset Owners:

In addition to the general requirement that each IAO is responsible for compliance with data protection legislation for their Service, they will also ensure that:

* their Service has compiled, and maintains, a process register
* their Service evidences its on-going compliance by regularly reviewing the relevant documentation, for example the process register, relevant policies, procedures, data sharing agreements and privacy notices
* their Service is aware for the need to carry out DPIAs along with the process for completing them, and carries them out when required
* their Service undergoes an annual Information Audit in order to assess compliance and to highlight areas that require improvement.

Failure to adhere to this policy and related procedures will be addressed in accordance with the Council’s Staff Disciplinary Procedures and relevant contractor and third party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

**Provisions of the Legislation**

The legislation regulates the processing of information relating to living persons in the UK. It requires that data controllers be registered with the UK Information Commissioner.

The Council is required to process all personal data held by it in accordance with the data protection principles contained within the legislation. The data protection principles state that data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
2. 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 not be considered to be incompatible with the initial purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. 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’);
5. 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);
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’).”

**Lawful Bases for Processing Personal Information**

The lawful bases for processing are set out in the GDPR. At least one of these must apply whenever the Council processes personal information, especially sensitive or special category data:

Consent: the individual has given clear consent for the Council to process his/her personal data for a specific purpose.

Contract: the processing is necessary for a contract that the Council has with the individual, or because the individual has asked the Council to take specific steps before entering into a contract.

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

Vital interests: the processing is necessary to protect someone’s life.

Public interest: the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council.

Legitimate interests: the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the Council in the performance of its official tasks; it can only apply to the Council when it is fulfilling a different role and carrying out a non-core activity.

**Individuals Rights**

GDPR provides individuals with the following rights regarding their personal information:

• The right to be informed about how their information will be used.

• The right of access to their personal information.

• The right to rectification, which is the right to require the Council to correct any inaccuracies.

• The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.

• The right to request that the processing of their information is restricted.

• The right to data portability.

• The right to object to the Council processing their personal information.

• Rights in relation to automated decision making and profiling.

The Council will publish information within Privacy Notices that will set out what these rights are and how these can be exercised.

**Subject Access Requests:**

The Information Governance Manager is responsible for subject access requests on behalf of the Council. This role will oversee the completion of all requests to the Council, with the exception of those received by the Children & Families and Health & Social Care Partnership sections which are responsible for processing those requests received.

Each individual employee is responsible for passing any subject access requests received to the Information Governance Team as soon as possible. The Council will endeavour to process all subject access requests within the statutory deadline of a month, unless an exemption to the time limit applies.

Under the new legislation there is no longer a fee applicable for a subject access request, other than where an exemption applies. The exception is where further copies of the original response is requested or the request is considered manifestly unfounded or excessive.

**Breaches:**

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to, personal data. Despite the security measures taken to protect personal data held by the Council, a breach or incident may occur.

The Council has a legal requirement to notify the ICO within 72 hoursof any personal data breach where it is likely to result in a risk to the rights and freedoms of data subjects.

An incident may occur in relation to the following:

Security

Individual’s rights

Used for purposes outwith reason for collection

Kept longer than necessary

Collecting more information than is needed

Not fair/legitimate/transparent/lawful

Kept accurate and up-to-date

Transferred outside EU without protection

Failure to notify the ICO of a breach may result in a significant fine being imposed.

It is the DPO’s responsibility to assess each personal data breach for consideration to report to the ICO and also has a duty to report any personal data breach to any affected data subjects. Therefore it is imperative all personal data breaches, both suspected, and confirmed, are reported immediately as required by the Data Breach procedures.

The DPO will ensure that Council management are regularly notified of any breaches or near misses that have been reported.

**Compliance:**

In order for the Council to comply with the legislation, it must carry out various tasks such as regular training, being transparent in personal data use, etc.

Services will undergo an annual information governance audit to ensure compliance with this and other policies and procedures.

**Training:**

The Council will provide advice and training for employees to comply with this policy. Additional guidance will be provided to staff who routinely handle personal, sensitive and confidential information.

Heads of Service are responsible for ensuring that employees within their Service are trained appropriately.

Mandatory training is required to be undertaken by all employees and Councillors every 2 years.

The DPO will assist Services in evaluating training need. Training materials will be developed in accordance with requirements.

**Retention & Disposal of Data:**

All personal information must be processed in compliance with the Council’s Records Management Policy and associated procedures to ensure that data is not retained for longer than it is required.

Personal data must be disposed of in a way that protects the rights and privacy of those the information is about, such as shredding, disposal as confidential waste and secure electronic deletion.

All systems should be reviewed on a regular basis to identify records which are no longer required and these will be destroyed in line with the Council’s records management policy.

A retention schedule will be developed in line with the Records Management Plan.

**Data Sharing:**

All sharing of data with other organisations must be appropriately documented for example with a Data Protection Impact Assessment completed, where relevant, and Data Sharing Agreement in place before any data is shared.

Information sharing within the Council across Service areas must also be documented with an agreement completed, and assessment where necessary.

**Information Security:**

All staff and elected members are responsible for ensuring that personal information which they hold is kept safe and secure. For more information please view the [Information and Communication Technology Security and Safe Use Policy](https://onedundee.dundeecity.gov.uk/document/information-and-communication-technology-security-and-safe-use-policy).

**Related Policies/Procedures:**

[Information and Communication Technology Security and Safe Use Policy](https://onedundee.dundeecity.gov.uk/document/information-and-communication-technology-security-and-safe-use-policy)
[Records Management Policy](https://www.dundeecity.gov.uk/sites/default/files/publications/Records%20Management%20Policy%20v2.1.pdf)
Data Sharing Policy
Data Security Classification Policy
DPIA Procedure
Data Breach Procedure
Subject Access Procedure

**Issue & Review:**

Heads of Service shall ensure that this policy is cascaded to all employees within their Service for it to be read and understood.

This policy will be reviewed every year and amended as appropriate.