Clackmannanshire Council | Comhairle Siorrachd Chlach Mhanann

www.clacks.gov.uk

DATA PROTECTION POLICY

Version:	1
Author/Service:	Legal & Governance Service – Heather Buchanan
Authorised by:	Head of Partnership & Performance
Release Date:	Approved by Partnership & Performance Committee 13/1/22 and ratified by a Meeting of Clackmannanshire Council on 10/2/22.
Policy Review Date:	1 December 2022

Revision History:

Revision Date	Revised by	Previous Version	Description of Revision
30 Nov 2021	Heather Buchanan		Policy revised to ensure compliance with the UK GDPR

Introduction

Clackmannanshire Council needs to collect, store, process and when required share information or data about people with whom it has contact in order to carry out its functions as a Local Authority and/or meet its statutory obligations.

The Council may need to hold personal data on a wide variety of individuals such as members of the public, customers and clients, elected members, past, present and prospective staff as well as suppliers of goods and services in order to fulfil its commitments.

This Policy applies to our processing of personal data of data subjects, and sets out how the Council will protect the rights of individuals and comply with the data protection legislation.

The Council recognises that it is essential to deal both legally and competently with personal data while conducting its day-to-day business. This creates a level of confidence between the Council and the people whose information it holds and demonstrates that the Council respects the privacy of those people. Clackmannanshire Council is exposed to potential fines for failure to comply with the provisions of data protection legislation.

This policy is not a stand alone document and should be read in conjunction with other related policies, procedures and guidance.

To comply with data protection legislation all employees, elected members, consultants, volunteers, contractors and other agents of the Council who use its computer facilities or paper files to hold and process personal information must comply with the Data Protection Policy.

Definitions

'Personal Data' means information relating to a living individual (the data subject) who can be identified from the data or from the data and other information which is in the possession of (or is likely to come into the possession of) the data controller.

'Special Category Data' means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometric information (where used for ID purposes), and information relating to an individual's health, sex life or sexual orientation.

'Data Controller' is a person or organisation who decides how any personal information can be held and processed, and for what purposes. Clackmannanshire Council is a Data Controller.

'Data Processor' – this role is carried out by a person other than a Council employee (for example a Contractor) who process personal information on behalf of the Council.

Purpose

The purpose of this policy is to ensure that the Council fully adheres with its legal obligations as set out in the UK General Data Protection Regulation (GDPR) and other data protection legislation in relation to the protection of personal data that it holds about any individual.

In complying with the Principles of Data Protection as laid down by GDPR the Council not only protects itself but also staff, customers and others who have contact with the Council. However, both the Council and individuals may be held accountable by the Information Commissioner's Office (ICO), the body which oversees the data protection laws.

Data Protection Principles

We will comply with the following six principles when processing personal data in carrying out our activities and functions as a Council. The personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

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.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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.

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.

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.

Data Protection Officer

The Council is required to have a named individual as the person with the overarching responsibility for ensuring compliance with the data protection legislation and promotion of good practice throughout the organisation.
The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Council and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor compliance with the GDPR and other data protection laws, including the assignment of responsibilities, managing and responding to data breaches, 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.

- Liaise and cooperate with the Information Commissioner's Office on issues related to the processing of personal data.

In addition to the above the DPO will also assist in determining the lawful basis for processing personal data, preparing appropriate contracts in terms of data sharing agreements, and handling complaints from data subjects.

Employee Responsibility

Each member of staff who deals with personal data has a responsibility to follow the procedures and guidelines set down by the Council in relation to data protection in order to ensure that data is held securely; not disclosed to any unauthorised parties and that it is disposed of securely once it is no longer required to be kept.

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

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Failure to comply with the Data Protection Policy can put at risk the data subjects whose personal data is being processed, and carries the risk of civil and criminal sanctions for the Council

Personal Data Breaches

A data breach may take many different forms, for example:

- Loss or theft of information or equipment on which personal data is stored.

- Unauthorised access to or use of personal data either by a member of staff or a third party.
- Loss of personal data resulting from an equipment or systems failure.
- Human error such as accidental deletion or alteration of personal data.
- Unforeseen circumstances such as a fire or flood.
- Deliberate attacks on our IT systems, such as hacking, viruses or phishing scams.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office without undue delay and, where possible, within 72 hours of becoming aware of the breach, if it is likely to result in a risk to the rights and freedoms of data subjects . A data subject must be notified if a data breach is likely to result in a high risk to their rights and freedoms.

Staff are required to contact the Data Protection Officer and their line manager immediately on the discovery of a potential data breach.

Retention of data

Personal data will be kept securely and should not be retained for longer than is necessary.
In order to comply with various legal requirements, Clackmannanshire Council is required to retain data it holds for differing lengths of time.

Once the data is no longer required to be held it must be securely destroyed. Information on the retention periods can be found in the Council's retention policy.

The rights of individuals

The General Data Protection Regulation provides individuals with the following rights regarding how we process their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information known as a subject access request.
- 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.

Lawful Processing

The Council must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual. These are:

- **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 or for the protection of the vital interests of the data subject or another person.

- **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

Where special category data and/or criminal offence data is processed the Council also need to identify a lawful condition for processing that information and document it.

The Council must include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices.

Privacy by Design

Data protection impact assessments (DPIAs) help the council to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. These should be carried out whenever a service is introducing a new system or where processing of personal data is likely to result in a high risk to the rights and freedoms of individuals.

Privacy Notices

We will issue Privacy Notices from time to time informing data subjects about the personal data that we process about them, how they can expect their personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Transfers of personal data outside the UK

We may only transfer personal data outside the UK on the basis that the recipient country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has adequate safeguards in place so far as data protection is concerned. Further advice can be obtained from the Data Protection Officer.

Other Policies, Procedures and Guidance

Staff Guide on GDPR
Data Breaches
Subject Access Requests
Data Security Policy
Data Protection Impact Assessments
Data Sharing

Online training on Data Protection – an introduction to GPDR

Further information and guidance

Any questions or concerns about this Policy should be directed to the Data Protection Officer,

Data Protection Officer
Clackmannanshire Council
Kilncraigs
Alloa
FK10 1EB

Email: dpo@clacks.gov.uk

Further information is also available from the Information Commissioner's website: www.ico.org.uk