Appendix 1

STIRLING COUNCIL

DATA PROTECTION POLICY

Service:	**Governance**	**Author:**	**Julia Mountford**
Approval body:	**Finance Economy & Corporate Support Committee**	**Date:**	**17 November 2022**
Version:	**1.0**	**Next revision due:**	**November 2024**

Contents

1. Introduction

Stirling Council (the "Council") provides a wide range of services to people who live, work, visit and invest in Stirling. To deliver services effectively the Council needs to collect, process and hold, large volumes of personal data.

Personal data is anything which is capable of identifying a living individual. Examples include names, addresses, identification numbers, CCTV images, telephone call recordings, e-mail addresses, location data, postcodes and photographs. Stirling Council also holds special category data. This is a class of personal data detailing racial and ethnic origin, political opinions, religious beliefs, physical and mental health, biometric data, sexual life and trade union membership and proceedings.

In addition, as a public authority, the Council has a legal obligation to appoint a Data Protection Officer ("DPO"). The role of the DPO primarily involves assisting the organisation to monitor internal compliance, inform and advise on data protection obligations, provide advice on Data Protection Impact Assessments and to act as a point of contact with the Information Commissioners Office (the "ICO").

The Council has a responsibility to safeguard the security of all personal data which it holds and has access to.

2. Purpose and Scope

This data protection policy (the "Policy") provides a framework for ensuring that Stirling Council meets its obligations under the UK General Data Protection Regulation and the Data Protection Act 2018 (the "UK GDPR" and the "DPA 2018", together the "DP Legislation"). The Policy is applicable to all personal data held by the Council irrespective of whether the information is held or accessed on Council premises or accessed remotely via mobile or home working. Personal information held on removable devices and other portable media is also covered by this Policy.

This Policy covers all processing of personal data carried out by Stirling Council and applies to all employees, elected members, third party suppliers and any other individuals with access to the Council's information and information systems.

The Council is obliged by law to document how it processes special category data and criminal convictions data within an Appropriate Policy Document. Please refer to the separate Appropriate Policy Document for more information on how special category and criminal offence data is handled.

3. Data Protection Principles

The DP Legislation sets out the seven key data protection principles which the Council must adhere to. These principles require that personal data is:-

- processed lawfully, fairly and in a transparent manner;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- not kept for longer than is necessary; and
- processed in a manner that ensures appropriate security.

In addition to the six principles above, the seventh principle is accountability, which requires Stirling Council to be able to evidence compliance with the six principles and make sure that individuals are not put at risk as a consequence of the processing of their personal data. Failure to evidence compliance can result in a breach of legislation and reputational damage, which may lead to financial penalties imposed by the data protection regulatory body, the ICO.

There is further guidance on these principles in the Council's Personal Data Supporting Guidance (the "DP Guidance").

4. **The Role of the DPO**

As highlighted in the introduction, the Council is under a legal duty as a public authority to appoint a DPO. This is an important role and the position of DPO is required to ensure that:

- The DPO reports directly to the highest level of management and is given the required independence to perform their role;
- The DPO is involved with all matters relating to the protection of personal data in a timely manner; and
- The DPO is not penalised for performing their duties

The primary role of the DPO is to ensure that the Council complies with DP Legislation. This includes ensuring that employees are aware of the Council's obligations to comply with DP Legislation, in addition to monitoring compliance with all internal processes and policies, and ensuring that all employees are sufficiently trained.

In recognition of the importance of the role, the DPO is appointed by the Chief Officer – Governance, has a direct reporting line to that post holder and must escalate any serious data protection concerns to them.

5. **Process and Procedure**

The Council is committed to ensuring compliance with the data protection principles. The Council will:-

- Ensure the fair collection and use of personal data;
- Have appropriate privacy notices in place;
- Only collect and process appropriate data, and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of the data used;
- Adhere to strict retention policies to determine the length of time the data is held;

- Take appropriate technical and organisational security measures to safeguard personal data;
- Ensure that personal data is not transferred outside the United Kingdom without suitable safeguards in place;
- Ensure that everyone managing and handling personal data is appropriately trained and supervised; and is fully aware of their data protection responsibilities;
- Regularly review and audit internal data handling processes and procedures;
- Assess processing of personal data perceived to be high risk by carrying out a Data Protection Impact Assessment (DPIA); and
- Ensure that the rights of data subjects can be fully exercised under the DP Legislation. These include:

    - The right to be informed that processing is being undertaken;
    - The right of access to their personal data;
    - The right to correct, rectify, block or erase data which is regarded as incorrect;
    - The right to restrict processing in certain circumstances;
    - The right to request data portability;
    - The right to object to certain processing, including the right to prevent processing for direct marketing; and
    - Rights to prevent automated decision making

The Council has a dedicated Records & Information Governance Team to ensure that the rights of data subjects are respected; this includes clear processes to handle subject access requests and other information right requests. Please read the DP Guidance for more information.

6. Data Sharing

Appropriate information sharing agreements and protocols must be agreed and put in place for instances of one-off sharing as well as planned and regular sharing of personal data between the Council and other partners. These will be reviewed, amended and updated on a regular basis in accordance with operational requirements.

7. Responsibilities

The Council has responsibility for demonstrating data protection compliance within the organisation.

Managers are responsible for ensuring that their staff are aware of this Policy and for developing and encouraging robust information handling practices.

All employees, elected members, and any other individuals with access to the Council's information must be familiar with the requirements of the DP Legislation and have a responsibility to ensure that personal data is properly protected at all times.

Employees will only have access to personal data where that access is necessary to enable them to undertake work duties. Access rights must not to be regarded as

permanent and are subject to change at any time dependent upon the nature of the duties being fulfilled by an employee.

Employees should only record information about an individual which is relevant to the purpose or purposes for which the information is being collected, and should be aware that they may be required to justify what has been recorded and that all recorded personal data may be released as part of a subject access request.

For Stirling Council employees, compliance with the Policy and associated procedures are a condition of employment. Violations of the Policy, such as inappropriately disclosing personal data or destroying or concealing personal data to avoid disclosure may result in disciplinary action.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

All those within the scope of this Policy have a responsibility to report any observed or suspected breach of this Policy to the Council's DPO in the first instance.

8. Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which can be accidental or deliberate.

The Council will seek to avoid personal data breaches by:-

- having a positive and proactive approach to data collection and management;
- ensuring the protection of the information it collects;
- ensuring it is used and shared appropriately;
- ensuring data is actively managed to ensure it remains relevant and up-to-date; and
- ensuring it remains fully compliant with legislation and best practice guidance from the ICO.

The Council recognises that if a personal data breach is not addressed in an appropriate and timely manner, it can result in physical, material or non-material damage to individuals. Where personal data breaches do occur, the Council will, without undue delay, seek to contain any harm to individuals, investigate the breach, and report the breach to the ICO where appropriate.

The Council has a duty to report any personal data breach which is deemed reportable to the ICO within 72 hours.

All personal data breach incidents must be reported immediately by telephone 01786 233406 or e-mail to dataprotection@stirling.gov.uk. The DPO will decide whether a breach should be reported and will liaise with the Chief Officer – Governance in advance of reporting.

If you are unsure whether to report an incident or not, the data protection team can assist.

9. Training

Regular data protection training is mandatory for all Council employees and Elected Members. The training module "Data Protection Essentials" is available along with a

Toolbox Talk via MyLO. This module can be completed as many times as necessary for refresher training.

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

10. **References**

In addition to this Policy there are supporting policies, procedures and guidance. The documents listed below are all available on the Council intranet and should be read along with this policy;

Appropriate Policy Document (will be hyperlinked when uploaded to intranet)

Personal Data Supporting Guidance

Privacy Notice

Incident Reporting

Records Management

Subject Access Requests and Your Rights

Employee Code of Conduct

Information Security Strategy