PERTH & KINROSS COUNCIL

Data Protection Policy

In this policy, the term 'the data protection laws' means EU 2017/679 (the General Data Protection Regulation), the Data Protection Act 2018, any related legislation, and any other relevant legislation impacting on the privacy of personal data.

Specific terms, such as personal data, controller, processor and processing, within this policy are used with the same meaning and intent as defined in the data protection laws.

Scope

This policy will apply to all elected members, employees, agents and volunteers of Perth & Kinross Council.

Violations of this policy may result in disciplinary action for an employee, referral of an elected member to the Standards Commission, and may constitute a criminal offence.

This policy applies to all processing of personal data by the Council.

Statement of Policy

The Council has to process a large amount of personal data in order to conduct its business. We will take all reasonable steps to ensure that we comply with the data protection laws in doing so.

We will ensure that we have identified the legal basis for all processing of personal information carried out by the Council. We will inform individuals appropriately about the processing that we undertake and will make it clear to individuals what is happening with and to their personal data.

We will ensure that we identify and document the purpose(s) for which we are processing personal data.

We will also ensure that we only gather and process the personal data we need to achieve a specified purpose.

We will ensure that we identify how accurate the personal data needs to be and that we can maintain it appropriately.

The Council has a retention schedule that details how long information should be kept. We will ensure that personal data is kept no longer than is specified in the schedule.

The Council has a policy, standards and practices for the security of information which meet recognised government and national standards. We will ensure that personal data is held and processed in accordance with these at all times.

In addition, before we

- start to process personal data for a new purpose
- make changes to the reason we process personal data, or
- change the means we use to process personal data

we will carry out an assessment of the impact on data protection at the earliest possible stage in the planning process.

Roles and Responsibilities

The Council will appoint an officer to fulfil the statutory role of Data Protection Officer (DPO).

The Head of Legal and Governance Services is responsible for the development, maintenance, publication and administration of this policy, and for the development and provision of appropriate data protection training for the Council.

Service Senior Management Teams are responsible for all aspects of compliance with this policy and the data protection laws within their Service.

Elected members, employees, agents and volunteers are required to comply with this policy and the data protection laws.

Elected Members

Elected members will be given access to such personal data as is required to carry out their duties as members of the Council or its Committees. All Elected Members with access to personal data must be familiar with the requirements of the data protection laws and undertake any data protection training required by the Council.

Elected members will be given access to personal data to fulfil their role as elected representatives when officers are satisfied that the elected member is acting at the request of the individual. An appropriate mandate from the individual will be required to give an elected member access to special category data or large amounts of personal data.

Individual elected members will act as data controllers in their own right for the duration of their tenure in office and, as such, are responsible for their individual compliance with the data protection laws. The Council will administer their registration as data controllers and pay the statutory fee on their behalf. The Council will act as a data processor for the elected members and will prepare a standard contractual undertaking for the relationship. The Council will also make appropriate standard documentation available for elected members.

Elected members must, when their term of office expires or for some other reason they cease to be an elected member, arrange for the secure disposal, or transfer to their successor, of all personal information held by them or by support staff on their behalf. Where information is being transferred, the Head of Legal & Governance Services, in consultation with the DPO will make the necessary arrangements for the transfer.

Employees

Employees will be given access to such personal data as is required to carry out their duties, but should only access personal data when necessary to fulfil those duties. All employees with access to personal data must be familiar with the requirements of the data protection laws and undertake any data protection training required by the Council.

Employees should only record information about an individual that is relevant and should be aware that they may be required to justify what is recorded and be prepared for the information to be disclosed to the individual.

Any employee who is found to have inappropriately accessed, amended, deleted, disclosed, or otherwise processed personal data may be subject to investigation under the Council's disciplinary procedure, which may result in dismissal and possible legal action.

Contracts

Where an organisation processes personal data on behalf of the Council there must be a contract (this includes a Service Level Agreement) in place with the organisation that contains the Council's standard data protection clauses or equivalent clauses approved by the Head of Legal and Governance Services and the DPO.

The Council's Information Security Manager must be satisfied that the information security measures adopted by the other organisation are adequate before the contract is agreed.

Data Sharing

Data sharing occurs when personal data is passed to another organisation for its purposes (rather than, for example, the organisation processing the personal data on behalf of the Council).

An appropriate written agreement for the sharing of personal data (known as a data sharing agreement or information sharing protocol) must be in place before any systematic or large-scale personal data sharing takes place. The DPO must be consulted prior to any such agreement being made.

Services are responsible for retaining and maintaining these agreements. The DPO will maintain a register of the agreements.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be undertaken to identify and minimise the privacy risks of any new project or policy that will involve processing personal data. The lead officer for the project or policy will be responsible for ensuring that the DPIA is undertaken. The DPO will assist Services to identify the need for a DPIA, provide guidance for the assessment process, and make recommendations to ensure the Council's compliance with the data protection laws.

The DPO will maintain a register of completed DPIAs.

Data Protection Officer

The Data Protection Officer will

- develop the Council's strategic response to the data protection laws and provide technical and professional advice and guidance to support the Council to comply with the legislation
- monitor the Council's compliance with the data protection laws and Council policies and procedures, including the carrying out of audits and ensuring that responsibilities have been assigned and training provided to employees in accordance with the law and this policy

- provide advice to help the Council carry out assessments in connection with data protection compliance
- liaise as necessary with the Information Commissioner's Office, including reporting data breaches when appropriate

The Council will give the DPO independence to carry out these tasks, ensure the DPO is able to do them freely and impartially, and will provide the DPO with adequate resources to undertake them.

The Council will involve the DPO when making any decision that relates to, or will result in, the processing of personal data.

Governance

The Council's Policy and Governance Group will act as the forum for the consideration of any matters related to data protection policy. In particular, they will approve minor or non-material amendments to this policy. This policy will be reviewed at least every three years.

Services will identify lead officers for data protection. These officers will meet regularly with the Council's DPO to consider data protection practice and procedures.

All complaints about data protection matters received by the Council will be dealt with by the DPO.

The DPO will handle all requests to exercise data subject rights made to the Council.

All data breaches within the Council will be reported to, and investigated by, the DPO who will liaise with Service management about the breach, mitigating actions and recommendations.

The DPO will present a report on the Council's data protection compliance to the Council's Senior Management and the Scrutiny Committee annually or more frequently if considered necessary.