



Data Protection Policy

January 2018

We process personal data in order to provide a number of our services. We are registered with the [Information Commissioner's Office](#) (ICO) as a data controller.

We are committed to protecting personal data and complying with the Data Protection Act 1998 (the Act) and the 8 data protection principles.

In terms of our [Financial Regulations](#), the Chief Executive is responsible for ensuring that the requirements of the Act are complied with. However, to assist her, each Senior Manager is responsible for compliance with the Act within their areas of responsibility

Our 8 core commitments

1. We will ensure that proper policies and procedures are in place to ensure compliance with the Act, in particular in the areas of Information Security and Records Management.
2. We will ensure that all staff who handle personal data understand their responsibilities under the Act and receive appropriate training annually.
3. We will ensure that our information technology systems protect the availability, integrity and confidentiality of personal data.
4. We will ensure that we tell data subjects what we will do with their personal data, by the use of fair processing notices.
5. We will ensure that procedures are in place to deal with subject access requests in line with the Act, and that we uphold other rights of data subjects under the Act.
6. We will ensure that we only share personal data with other organisations when appropriate and that it is shared safely and securely. Information sharing agreements will be put in place where regular sharing takes place.
7. We will ensure that we include appropriate clauses in contracts with third parties where they process personal data on our behalf.
8. We will ensure that any data breaches are handled in line with the [ICO's guidance on data security breach management](#). All breaches will be recorded in a central log maintained by Falkirk Council's Chief Finance Officer, on behalf of the Trust. Any serious breaches will be reported to the ICO.

Compliance with this policy, and related policies and procedures, is a condition of employment.

This policy will be reviewed every 3 years.

Summary of data protection principles

1. Personal data must be processed fairly and lawfully.
2. Personal data must be processed for limited purposes.
3. Personal data must be adequate, relevant and not excessive.
4. Personal data must be accurate and up-to-date.
5. Personal data must not be kept for longer than is necessary.
6. Personal data must be processed in line with the data subject's rights.
7. Personal data must be secure.
8. Personal data must not be transferred to other countries without adequate protection.

Glossary

Data

Recorded information of any kind, including information held in a form which can be processed by computer.

Personal data

Data which relates to a living individual who can be identified (a) from that data or (b) from that data and other information in the possession of the data controller. This includes an expression of opinion about the individual.

Data controller

A person who determines the purpose for which, and the manner in which, any personal data are, or are to be, processed.

Processing

Includes obtaining, recording, holding, using, adapting, altering, disclosing, deleting or erasing.

Data subject

An individual who is the subject of personal data.

Subject access request

A written request by an individual to a data controller under section 7 of the Act, usually for any personal data processed by the data controller of which s/he is the data subject.