

Falkirk Council

Policy Statement on Special Category Data

Version 1.00



Falkirk Council

Falkirk Council – policy statement and additional safeguards on processing special category data and personal data relating to criminal convictions and offences

Introduction

With effect from 25 May 2018, data protection law requires controllers who process special category (i.e. sensitive) personal data, (or personal data relating to criminal convictions and offences) under various parts of the Data Protection Act 2018 to have an “appropriate policy document” in place setting out a number of additional safeguards for this data.

More specifically, the law states that:

The controller has an appropriate policy document in place in relation to the processing of personal data...if the controller has produced a document which—

- (a) explains the controller’s procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and
- (b) explains the controller’s policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained.

This document is the policy adopted by Falkirk Council and Licensing Board (together referred to in this policy as **Council**) in relation to this processing.

Policy Statement

1: Lawfulness, fairness and transparency

All data flows into and out of the Council have been assessed to determine the legal basis under which that data is processed and the results of the assessment are being documented. We are satisfied that we will have a legal basis for holding the personal data we hold, and that we will also have a valid legal basis for disclosing this personal data to third parties where this happens. Privacy notices have been drafted to comply with GDPR requirements (and to reflect the legal basis of processing). Please see www.falkirk.gov.uk/privacy for further details. We are presently updating our data processor agreements and data sharing agreements to reflect the new legal requirements where required.

2: Purpose limitation

The purposes for which data are collected are clearly set out in the relevant privacy notices. A limited set of data is required for internal management purposes, and research and archiving purposes.

3: Data minimisation

In assessing the data flows, the Council has taken the opportunity to assess the need for each of the data fields in question and where superfluous data was being captured, we have stopped capturing this.

4: Accuracy

The Council will, where any inaccuracies are discovered, ensure that these are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

5: Storage limitation

The Council only keeps personal information for the minimum period amount of time necessary. Sometimes this time period is set out in the law, but in most cases it is based on business need. We maintain a business classification scheme (which includes a records retention and disposal schedule which sets out how long we hold different types of information for. This is currently under review. Please contact us to ask for details of this. The Archives are held by Falkirk Community Trust on behalf of the Council subject to appropriate safeguards in terms of Article 89.

Ongoing management of the Council's records and information is subject to the provisions of our Records Management Plan, which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. It is available [online](#). The Records Management Plan sets out, in much greater detail, the provisions under which the Council complies with its obligations under public records legislation, data protection and information security and is complementary to this policy statement.

6: Integrity and confidentiality

The Council has an Information Security Policy in place which sets out roles and responsibilities within the organisation in relation to information security. This is currently under review. All staff are required to take data protection & information security training and this is refreshed annually. Our ICT systems have appropriate protective measures in place and systems are subject to external assessment and validation where required. We have detailed data protection and confidentiality guidelines in place which are reviewed annually.

Version Number	Purpose/Change	Author	Date
1.00	First draft	Information Governance Manager	17.07.18