



Falkirk Council
*Corporate & Commercial
Services*

**Falkirk Council
Data Protection
Guidelines**

Contents

Contents	2
Objectives	3
What does the Data Protection Act 1998 do?	3
Who is who under the Data Protection Act 1998?	4
Definitions	4
The Eight Principles of Data Protection	5
What does this mean to me?	6
Subject Access Rights	8
Data Protection & CCTV	8
Data Protection and Elected Members	9
Summary	10

Objectives

The objectives of these guidelines are to:

- provide general information on the main points of the Data Protection Act 1998
- outline the obligations of the Council – both employees and Elected Members – under the Data Protection Act 1998
- advise on the rights of the individual in relation to the processing of their personal data
- promote good practice within the Council in the handling of personal data
- outline the obligations of the Council in relation to the use of CCTV

What does the Data Protection Act 1998 do?

The Data Protection Act 1998 applies to the processing of data in relation to the living, identifiable individual and is there to protect personal privacy and uphold the rights of the individual.

The Act:

- Established the Office of the Data Protection Commissioner (now known as the Information Commissioner)
- Provides the rules for the notification process
- Sets out the rights of the individuals in respect of the processing of their personal data
- Provides the framework within which data controllers should process personal data – the Eight Principles of Data Protection
- Gives powers to the Commissioner to enforce the Act

Who is who under the Data Protection Act 1998?

Information Commissioner

This is the post established within the Act to oversee the implementation and enforcement of the Act. The Office of the Information Commissioner is set up to manage the notification process, to handle queries and complaints and to enforce the terms of the Act. This post is now known as the Information Commissioner as the post and office are to manage the enforcement of the Freedom of Information Act for England and Wales as well as Data Protection UK wide. It was previously known as the Data Protection Commissioner.

Data Controller

This is the organisation or individual(s) who hold and use (process) personal information. Data controllers are responsible for ensuring that data is processed within the principles of the Act.

Data Subject

These are the individuals about whom a data controller holds personal data. Data subjects have certain legal rights in relation to how, if at all, their personal data is processed.

Definitions

Certain words have specific meanings under the Data Protection Act 1998:

Processing

Obtaining, recording or holding of information/ data by carrying out an operation or set of operations on the information/data including the organisation, adaptation or alteration of information/data, retrieval, consultation or use of information /data, disclosure, combination, erasure or destruction of data.

Data

The Data Protection Act refers to data as meaning information that is:

- Automatically processed
- Recorded with the intention of being processed
- Recorded as part of a relevant filing system

Relevant Filing System

A relevant filing system is that which is structured in a way that specific information is readily accessible.

The Eight Principles of Data Protection

First Principle: *Personal data must be processed fairly and lawfully.*

There are two main conditions for meeting this principle – either that the data subject gives consent for the data to be processed or where the processing is necessary to fulfil legal or contractual obligations. For data to be processed fairly and lawfully, the data subject should be aware of who the data controller is and why the data is being processed.

Second Principle: *Personal data must only be obtained for one or more specified purpose(s) and must only be processed in a way that is consistent with the specified purpose.*

Data should only be collected by data controllers where there is a specific reason for doing so. The data subject must be advised of the purpose(s) for which the data is collected and the data must not then be used for another unrelated purpose e.g. data collected for the purpose of benefits administration must not be used to promote swimming lessons at the local pool without first seeking, and obtaining, consent from the data subject.

Third Principle: *Personal data must be adequate, relevant and not excessive for the purpose it was processed for.*

Only data that is needed to fulfil the purpose for which it is collected should be requested from the data subject. Data must not be collected simply because it might be useful in the future.

Fourth Principle: *Personal data must be accurate and, where necessary, kept up to date.*

Data controllers should take reasonable steps to check the accuracy of the information they both receive and hold. They should also ensure that data is kept up to date or, where appropriate, destroyed after a reasonable amount of time has elapsed.

Fifth Principle: *Personal data processed for any purpose must not be kept longer than is necessary to fulfil that purpose.*

Data controllers should not keep data for any longer than is required to fulfil the purpose for which it was collected unless there is a legal requirement to do so.

Sixth Principle: *Personal data must be processed in line with the data subject's rights.*

Data subjects have the right:

- To access data held about them

- To prevent processing where it is likely to cause substantial damage or distress to them or anyone else
- To be informed of the logic of automated decision-making processes to which their personal data has been subjected
- To refuse to allow a data controller to use their personal data for direct marketing purposes – even if the same data controller fairly and lawfully processes their personal data for another purpose
- To request that a data controller correct or destroy data which is inaccurate. (They can only ask for data to be destroyed where there is no legal obligation on the data controller to process the data e.g. the Inland Revenue can be asked to correct inaccurate data, but they must continue to process the data to fulfil a legal obligation.)

Seventh Principle: *Appropriate security measures must be taken to protect against unauthorised or illegal data processing.*

Data controllers are required to ensure that adequate security controls are in place within the workplace to protect personal data. The Office of the Information Commissioner recommends that data controllers should process data within the principles laid down in BS7799 – The British Standard on Information Security. This includes looking at password protection, physical and environmental factors surrounding both electronic and manual data storage, access and display, organisational security, staff training and security policies.

Eighth Principle: *Transferring personal data outside the European Economic Area is restricted unless the rights and freedoms of data subjects are protected.*

Countries outwith the European Economic Area may not have the same laws protecting the privacy of the data of the individual that those within it have. Data controllers must take steps to ensure that if data is transferred outwith the European Economic Area it is secure.

What does this mean to me?

On a day to day basis, there are a number of things which all employees and Elected Members should be aware of when dealing with personal data – data which, in the terms of the Act, relates to the living, identifiable individual.

- There should be an appropriate notification to the Commissioner for the purpose you are processing the data, the type of data you hold about the individuals and from whom you can source the data and to whom you can

disclose it. In the case of employees, the Data Controller is Falkirk Council and where Elected Members are processing data for their own or party purposes, it would be the member themselves or the Political Party which they represent.

- When personal data is collected, the form used for collecting it should clearly state who the data controller is, what purpose(s) the data is being collected for and if the data is to be passed to a third party who that is and the purpose they will process the data for.
- Data should never be used for a purpose it was not collected for without seeking the consent of the Data Subject.
- The Act covers paper-based records as well as those held on computer and extends to other media such as CCTV.
- There is a requirement for good, robust Records Management with appropriate retention schedules for different record types.
- Data should never be disclosed to a third party without seeking the consent of the Data Subject. Be careful when answering queries relating to personal information – especially over the phone. Always ensure that it is the Data Subject you are dealing with. It's better not to give out personal data at all if you are not sure to whom you are speaking.
- The police have powers under the act to access all data we hold for:
 - The investigation and detection of a crime
 - The apprehension of an offender
 - The collection of a tax or duty

But, like all requests, be wary of Police requests over the phone – always get these in writing-do not disclose over the phone.

- The eight principles should always be adhered to when processing personal data.

Subject Access Rights

Any data subject has the right to access personal data held about them by a data controller. This includes:

- The purpose(s) for which the data is processed
- The type of data held e.g. name, address, NI number etc.
- From whom the data is sourced
- To whom the data is disclosed

The Subject Access request must be in writing and the Data Controller has 40 days to respond to the request. Care must be taken to ensure that, in disclosing the data to the Data Subject, no personal data relating to a third party is made without the consent of the third party – even in the case of a husband and wife.

Data Protection & CCTV

The 1998 Data Protection Act widened the requirement to process personal data from that held on a computer, as in the 1984 Act, to cover both paper records and other forms of electronic storage of data including CCTV.

The requirements of the Act in relation to CCTV include:

- All CCTV system owners, where the CCTV covers an area of public access, are Data Controllers as defined in the Act and as such require to notify the Commissioner of the use of CCTV and the purpose it is used for.
- The eight principles of the Act apply to the processing of CCTV data as this is deemed to be the processing of the image of the living, identifiable individual.
- Signage must be erected at the edge of the area where the CCTV monitoring starts to notify the public their data is being processed. These should display the name of the Data Controller and give a daytime contact as well as the purpose for which the data is being processed.

- Cameras are only authorised to monitor areas owned by the Data Controller and covered by the appropriate signage.
- All personnel using the system should be trained in their use and made aware of their obligations under the Act.
- The CCTV monitors should not be in a public place and should only be viewed by trained and designated employees or agents of the Data Controller.
- Tapes require to be stored in a locked, preferably metal, container.
- Tapes require to be changed on a daily basis and kept for one month after recording, after which they should be de-guazed (wiped clean of data using electronic equipment) before re-use.
- Tapes require to be de-guazed and destroyed after 12 cycles of use (one year).
- Tapes should only be viewed for the purpose for which the data was processed.
- The same subject access rights apply to CCTV tape as to paper based and computer held data.

Data Protection & Elected Members

There are a number of Data Protection Issues directly relating to Elected Members.

- Elected Members collecting and processing personal data in their own right e.g. from their surgeries and then storing this information on a computer, will have to undertake the process of notification with the Information Commissioners Office to fulfil the 'fair and lawful collection' principle.
- Elected Members must ensure that constituents who provide them with personal data are made aware that the information will be passed to relevant Officers of the Council and may, in certain circumstances, be passed to the Convenor of the appropriate

Committee. If the constituent does not consent to this transfer of data, the Elected Member then requires to do two things:

1. Advise the constituent that this may mean that their complaint cannot be properly handled.
 2. Obtain a letter from the constituent confirming who may or may not have access to their data.
- Where a member of the public approaches an Elected Member who is not their Ward Councillor they should be informed that the information and any replies will be copied to their Ward Councillor. The constituent has the right to ask for this not to be done, and, as the Elected Member who was approached is the Data Controller, they would not then be able to pass the information to a third party as consent was not given by the data subject.

Summary

Everyone who deals with personal data in their business, regardless of their occupation and designation requires to be aware of the Data Protection Act 1998.

By adhering to the Eight Principles of the Act when processing – and by definition this means carrying out almost any operation in relation to – personal data and sticking to the rules they provide ensures that we comply with the Act.

Contact

If you require more information about the Act or these Guidelines, please contact either Legal Services or Heather Robb in ICT on 501584.