



Data Protection Policy

Co-ordinator	Will Taylor
Date of Completion	June 2017
Date of adoption by Governors	June 2017
Date to be reviewed	June 2019

Introduction

The new Data Protection Act 1998 (EU Directive 95/46/EC) came into effect on the 24th October 1998 and was brought into force on March 1st 2000. The new Act relates to a wide range of personal data, not just that held in computer systems. It now includes data held in manual filing systems, video and closed circuit television images (CCTV).

Purpose

The purpose of the Act is to protect the rights of individuals (data subjects) when data is obtained, stored, processed or supplied to others.

Data subjects (individuals) may obtain information held about themselves, challenge it if appropriate, have inaccurate information changed or deleted and claim compensation in certain circumstances.

The Act places obligations on all those who record and use personal data (data controllers), such as the Council, to be open about that use by:

- registering/notifying all uses of personal data with the Office of the Information Commissioner (formerly the Data Protection Registrar)
- following sound and proper practices (the Data Protection Principles).

Scope

Data Protection is the responsibility of all members of Brighton & Hove City Council staff.

We all have access to personal data and we must individually ensure that it is processed according to the Data Protection legislation.

Registration/Notification

The Council has to make sure that all personal data and the uses to which it is put (including disclosure in any form to third parties) is notified/registered in a national register maintained by the Information Commissioner.

The Data Protection Principles

Registered data controllers (i.e. Brighton & Hove City Council) must comply with the following eight Data Protection Principles in relation to the personal data they hold:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purpose.
- Personal data shall be adequate, relevant and **not excessive** in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.

Data Protection Act 1998 Policy

- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Security measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Information Commissioner

The Information Commissioner administers the Data Protection Act. The role and duties of the Commissioner include:

- ensuring compliance with the Act
- ensuring that individuals rights to privacy are respected
- ensuring that individuals have access to data held about themselves
- establishing and maintaining a Register of data users and making it publicly available
- investigating complaints, serving notices on registered data users who are contravening the principles of the Act, and where appropriate prosecute offenders.

The Act gives the Information Commissioner wide powers to ensure compliance with the Act, including warrants to search and seize documents and equipment.

Access to Data - (Subject Access)

If individuals want to see information held by the Council about them, they must write to ask for that information. Subject to certain exemptions they will be entitled to a copy of all the personal information held about them. The authority can charge a fee for this service.

Individual's requests have to be processed within **forty calendar days** of receipt of the request. Brighton and Hove City Council's internal timescale is **twenty-one calendar days**. All such requests must be referred to the Information Governance Office (01273 296487) or the Data Protection Manager (01273 291207) to make sure that correct procedures are followed.

Disclosure of Personal Data

The Council can disclose information about an individual, provided that it has complied with the Data Protection Principles and the registration requirements i.e.

- the person to whom the disclosure is made is described in the disclosures section of the data user's register entry, or
- the disclosure is covered by one of the 'non-disclosure exemptions'.

Thus individuals have no general right to object to the disclosure of personal data relating to them.

However, the first Data Protection Principle requires the Council to obtain and process information fairly and lawfully. Employees should be careful not to deceive or mislead anyone, even inadvertently, about the purpose for which information is to be held, used or disclosed.

Care should be taken to ensure that in disclosing personal information employees do not breach any duty of confidence, exceed the Council's statutory powers or otherwise act unlawfully. All such disclosures must of course be compatible with the relevant corporate and departmental policies for the disclosure of the particular categories of information concerned.

Data Protection Act 1998 Policy

Managers writing staff references must not include reasons for staff absence. They may disclose the number of days a member of staff has had off sick, but not the ailment suffered by the member of staff as this is deemed to be sensitive personal information.

Exemptions

There are exemptions to the Act which may be applicable in certain defined circumstances.

Advice must always be sought from your departmental Data Protection Liaison Officer on the application of these exemptions.

Responsibilities

Employees have a responsibility to ensure that they comply with the Act themselves and encourage others to do so. They and in particular their managers are responsible for ensuring that all personal information in use which is subject to the Act is properly registered.

Information Officers are responsible, within their departments for providing advice and guidance, ensuring registrations are kept up to date, ensuring corporate requirements are met and all relevant aspects of the Act are complied with within their departments.

The Council's ICT Partnership Manager is responsible for co-ordinating all Data Protection activities within the authority, helping and advising departments, monitoring compliance with the Act and acting as the point of contact with the Office of the Information Commissioner.

Non-Compliance with the Requirements of the Act

The Act creates a number of criminal offences which include:-

- Holding personal data without being registered or without having applied for registration
- Knowingly or recklessly:-
- holding personal data not described in the register entry
- using, obtaining, disclosing or transferring personal data other than as described in the register entry
- operating as a computer bureau in respect of personal data without being registered as such
- supplying the Information Commissioner with false or misleading information on an application for registration or for alteration of a register entry.

The Council (as Data Controller) and its employees or agents could be prosecuted for contravening the requirements of the Act.

Internet/Intranet

Any personal data that is obtained from, or used for the Internet/Intranet, **must** be fully compliant with the eight principles of the Data Protection Act 1998.

Consent must be obtained from individuals before any information (including photographs or e-mail addresses) is published or disclosed about them. There is an exception to this - when an individual has already placed information about themselves in the public domain, such as the author of a book. Their names can be published without having to obtain consent e.g. a list of books available in a library.

Data Protection Act 1998 Policy

When information is obtained from individuals they must be clearly informed that the information they provide will be made publicly available worldwide via the Internet. Information that has been obtained for one purpose must not be used or disclosed for any other purposes, without the individual's consent, or giving them the opportunity to opt out from it.

Contacts

Council's Data Protection Officer

Data Protection Manager	-	Jan McCartney	01273 291207
Information Governance Officer	-	Adam Rezazadeh	01273 296487

Office of the Information Commissioner

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF