

Policy Documents**Data Protection Policy****Information Systems Policies****Data Protection Policy****Version : 1.0****Date Released : 3 July 2001***Document Identification & Status***Title** Data Protection Policy**Document Reference Number** ABCIT-POLICY-001**Owner** Rob Neil, Head of Corporate ICT*Document History*

<i>Version</i>	<i>Date</i>	<i>Description</i>
0.1	18 th June 2001	First Draft

*Document Release Authorisation***Name** Rob Neil**Role** Head of Corporate ICT**Release Date****Signature****Ashford Borough Council****Data Protection Policy**

1. Data Protection Policy

The processing of Personal Data by Ashford Borough Council will comply with the UK Data Protection Act 1998, which implements within the UK the requirements of the EC Data Protection Directive [EC/95/46]. The basic requirement is that the processing, both automated and manual, should comply with the following Data Protection Principles which require that Personal Data shall:

- be processed fairly and lawfully
- be obtained only for specified and lawful purposes, and not be processed in any incompatible manner
- be adequate, relevant and not excessive
- be accurate and, where necessary, kept up to date
- not be kept for longer than is necessary
- shall be processed in accordance with the rights of Data Subjects
- be protected by appropriate security measures
- not be transferred outside the EEA unless adequate level of data protection exist.

Therefore, Ashford Borough Council will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom information is held, are able to be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.);
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards.

Ashford Borough Council will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anybody wanting to make enquiries about handling personal information knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are clearly described;
- A regular review and audit is made of the way personal information is managed;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated.

1. Data Security

The security of the Personal Data processed by Ashford Borough Council will be at the level of BS7799 although the organisation will not be certified to BS7799.

2. Data Controller

For practical purposes all communications, queries and Subject Access Requests which relate to Data Protection issues should be addressed to the Data Protection Officer, for action or response on behalf of Ashford Borough Council.

The Data Protection Officer

Ashford Borough Council

Civic Centre

Tannery Lane

Ashford

Kent

TN23 1PL

Email: dpo@ashford.gov.uk

Data controllers brief guide

The Data Protection Act: A brief guide for data controllers

Introduction

The growth in the use of personal data has many benefits both, for society, like helping to fight crime and for the individual, like better medical care. However, whenever personal data are collected and used, people's lives can be adversely affected if something goes wrong. For example, if details are not entered correctly people can be unjustly refused credit, benefits, housing, or even a job. If data are not kept securely, people's privacy can be affected. It is vital that those who collect and use personal data maintain the confidence of those who are asked to provide it by complying with the requirements of the Data Protection Act.

The Data Protection Act 1998 came into force on 1 March 2000. It sets rules for processing personal information and applies to some paper records as well as those held on computers.

The Data Protection Act in practice

The Data Protection Act applies to 'personal data' that is, data about identifiable living individuals. Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

The rules of good information handling - the principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in line with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual.

Processing personal data

'Processing' is broadly defined and takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed "fairly and lawfully". Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject must be told the identity of the data controller and why that information is or is to be processed.

Processing may only be carried out where one of the following conditions has been met:

- the individual has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- the processing is necessary to carry out public functions;
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

Processing sensitive data

The Data Protection Act makes specific provision for sensitive personal data. Sensitive data include: racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions.

Sensitive data can only be processed under strict conditions, which include:

- having the explicit consent of the individual;
- being required by law to process the data for employment purposes;
- needing to process the information in order to protect the vital interests of the data subject or another;
- dealing with the administration of justice or legal proceedings.

Paper files

The Data Protection Act covers information which is recorded as part of a 'relevant filing system', that is, a set of information in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that 'specific information relating to a particular individual is readily accessible'. The definition means a significant amount of manual data falls under the scope of the Data Protection Act, as does the extension of the definition of data to cover 'accessible records'. Accessible records are broadly: school pupil, housing, social services and health records to which access was previously available under other legislation.

Transitional arrangements will exempt manual records held in a "relevant filing system" before 24 October 1998, from full compliance until 2007. However, the right of subject access to information held in paper files covered by the Data Protection Act is available from 24 October 2001 regardless of the date from which the information was held.

Security

Data controllers must take security measures to safeguard personal data. The 1998 Act requires that data controllers must take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of data. Where a controller uses the services of a data processor the security arrangements must be part of a written agreement between the two.

Transfer of Personal Data Overseas

The eighth principle restricts the transfer of personal data outside the EEA (which consists of Norway, Iceland and Liechtenstein as well as the 15 EU Member States). Personal data may only be transferred to third countries if those countries ensure an "adequate level of protection for the rights and freedoms of data subjects".

Notification

Most data controllers will need to notify the Commissioner, in broad terms, of the purposes of their processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register. Notification is not linked to

enforcement. Under the 1998 Act all data controllers must comply with the data protection principles, even if they are exempt from the requirement to notify. Data controllers have a single register entry. Notifications are renewable annually.

Transitional Relief

Processing already under way before 24 October 1998 will be eligible to claim transitional relief from the additional requirements introduced by the 1998 Act until 23 October 2001. Data held in accessible records are exempt from the requirements of the data protection regime, except for subject access and rights to compensation for inaccuracy, until 23 October 2001.

The rights of individuals

The right of subject access

The Data Protection Act allows individuals to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access.

The right of rectification, blocking, erasure and destruction

The Data Protection Act allows individuals to apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

The right to prevent processing

A data subject can ask a data controller to stop or request that they do not begin processing relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.

The right to prevent processing for direct marketing

A data subject can ask a data controller to stop or not to begin processing data relating to him or her for direct marketing purposes. This is an absolute right.

The right to compensation

A data subject can claim compensation from a data controller for damage or damage and distress caused by any breach of the Data Protection Act. Compensation for distress alone can only be claimed in limited circumstances.

Rights in relation to automated decision-taking

An individual can ask a data controller to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this.

Telecommunications

The Telecommunications Regulations 1999 (Data Protection and Privacy) imposes special rules for dealing with data in public telecommunications systems, faxes, telephones, and automated calling systems for unsolicited marketing.

- Unsolicited marketing faxes must not be sent to individual subscribers without their prior consent.
- Individual subscribers have a statutory right to opt-out of unsolicited telephone marketing either by telling the caller or by registering on a central stop list.
- Corporate subscribers cannot opt-out of telephone sales but have the right to opt-out of unsolicited marketing faxes.
- Automated calling systems must have the prior consent of both corporate and individual subscribers.

Criminal Offences

Notification offences

These are committed where processing is being undertaken by a data controller who has not notified the Commissioner either of the processing being undertaken or of any changes that have been made to that processing. Failure to notify is a strict liability offence.

Procuring and selling offences

It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also an offence to access personal data or to disclose it without proper authorisation. This covers unauthorised access to and disclosure of personal data. There are some exceptions to this.

Enforced subject access offence

Unless one of the limited statutory exceptions apply, it is an offence for a person to ask another person to make a subject access request in order to obtain personal data about that person for specified purposes, such as a precondition to employment.

Other offences

It is an offence to fail to respond to an information notice or to breach an enforcement notice. Unauthorised disclosures by the Commissioner or her staff are forbidden and breach of those provisions is an offence.

Created by

Norman Orchison

Created

Tue, 09 Oct 2001