



BISHOPS WALTHAM MEN'S SHED

Data Protection and the Data Protection Act 1998

The Data Protection Act 1998 (the "Act") governs the collection, recording, storage, use and disclosure of personal data whether such data is held electronically or in manual form. Young people have the same rights as adults under the Act.

1. THE MAIN PURPOSE OF THE ACT

The Act aims to protect the individual's right to privacy by promoting high standards in the way personal information about that individual should be handled. The rules apply to personal information held electronically incl. email, word documents, in a database, etc. or held manually in a readily accessible filing system. The Act provides two main ways by which this is achieved:

Firstly, any 'data controller' who 'processes' 'personal data' about a living individual must observe the eight 'Data Protection Principles' enshrined in the Act. The Act further classes particular data as 'sensitive personal data' and provides additional rules for processing this.

Secondly, all 'data subjects' i.e. individuals about whom personal data is held, are given wider 'rights of access and control' in relation to it.

2. DATA CONTROLLERS AND THE RULES REGARDING PERSONAL DATA

A 'data controller' is any individual, group or organisation, established in the UK processing personal data about an individual (who can then be identified from that data). The Act does not apply to individuals collecting information solely for their own domestic and household affairs e.g. an address book or solely for research, journalistic, artistic or literary purposes.

The Act also only applies to 'personal data', which is essentially any significant piece of information about a living, identifiable individual e.g. a name together with an address, age, telephone number, information regarding his/her hobbies etc. It can also include an expression of an opinion about that individual. A data controller controls the purpose and method of processing such personal data (this is different than a 'data processor' who merely processes data on a controller's behalf).

'Processing' is given a wide meaning and includes obtaining, recording, holding, altering, retrieving, destroying or disclosing data.

The 8 'Data Protection Principles'

Under the Act, all data controllers must apply the following 8 'Data Protection Principles', which state that personal data must be:

1. Processed fairly and lawfully;
2. Obtained for a specified and lawful purpose;
3. Adequate, relevant and not excessive to that purpose;
4. Accurate and up-to-date;
5. Kept only for as long as required for the purpose for which it was obtained;
6. Processed in accordance with the rights of data subjects;
7. Be kept secure proportionately to the level of harm that could result if unauthorised access occurs;
8. Not transmitted outside the organisation without consent from the data subject.

Additional rules for 'Sensitive personal data'

The Act further categorises certain personal data as 'sensitive personal data' and imposes additional rules about handling this. The data controller must first obtain the explicit consent of the data subject in order to obtain and hold such information. Personal data becomes 'sensitive' if it includes information as to:

- a) Racial or ethnic origin; or
- b) Political opinions; or
- c) Religious beliefs; or
- d) Trade union membership; or
- e) Physical or mental health; or
- f) Sexual life; or
- g) Commission of offences or alleged offences.

However, explicit consent is not required where the data subject has already publicised the data e.g. for: Medical purposes; Legal proceedings; Monitoring racial equality; or Employment purposes.

3. DATA SUBJECTS AND THEIR RIGHTS

Following a request in writing to the data controller, a data subject is entitled (with some exceptions) to a description and a copy of personal data being held or being processed about them together, with an explanation as to why it is being processed/held and to whom it has been disclosed. The data controller may charge a standard fee to the data subject (a maximum of £10) and must comply with the request within 40 days.

Data subjects can have inaccurate data rectified, erased or destroyed and can stop data from being processed if it is unnecessary or causing damage or distress

A data subject may not be entitled to this right if they have already consented to the processing of their personal data (although such consent can be revoked) and also where such processing is necessary to perform a contract to which the data subject is a party to e.g. employment contract;

Comply with a legal obligation;

Protect the vital interests of the data subject; Make a request to the Information Commissioner's Office (ICO) to assess whether the Act has been contravened.

Dealing with a data subject's request

If a BWMS receives a request in writing from a data subject for a description and copy of personal data held about them, the request should be acknowledged and the person appointed must comply with the request within the 40-day time limit.

If there is a risk that another individual will be identified from disclosing the data, the request may be refused unless that other individual has consented or it is possible to blank out the other individual's particulars so they are no longer identifiable from the information. Such instances will need to be considered carefully on a case-to-case basis.

GLOSSARY OF IMPORTANT TERMS

“data controller”

The person or persons who determine the purposes and manner in which personal data is processed.

“data processing”

Includes the obtaining, recording, storing, using and the disclosing of personal data.

“data processor”

Any individual, group or organisation who processes data on behalf of the data controller (not being an employee of the data controller).

“data subject”

Each living individual whose information is held.

“personal data”

Data about any living individual who can be identified from that data or from any other information held by the data controller including expressions of opinion by or about the data subject.

“sensitive personal data”

Information as to an individual's racial or ethnic origin, political opinions, religious or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life or commission or alleged commission of any offence and/or sentence of any court.