**Data Protection Policy**Note: Drafting issues

**Drafting issues**

**Drafting issues**

This policy is drafted for use by businesses operating in the UK to set out the conditions under which they process personal data of their employees, customers, suppliers and other third parties. Data protection policies are not specifically required under the DPA, but they can help businesses to ensure compliance with the Act. Failure to comply can, in certain cases, lead to criminal sanctions (with directors and other company officers potentially facing personal liability) and liability for damages, not to mention negative publicity (see [*Practice note, Data protection issues on commercial transactions (www.practicallaw.com/5-200-2146)*](http://employment.practicallaw.com.lawdbs.lawcol.com/5-200-2146)).

[Hide Note](http://employment.practicallaw.com.lawdbs.lawcol.com/9-379-8623?q=data+protection+policy#null)

**1. POLICY STATEMENT**

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff and our clients, and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, clients, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

**2. STATUS OF THE POLICY**Note: Status of the Policy

**2. Status of the Policy**

**Status of the Policy**

It is not compulsory for the business to appoint a data protection compliance manager but it will be useful, particularly in larger companies, if the administration and oversight of the company's data protection regime is in the hands of a single individual who has received adequate training in the legal and commercial issues surrounding data protection law.

[Hide Note](http://employment.practicallaw.com.lawdbs.lawcol.com/9-379-8623?q=data+protection+policy#null)

2.1 This policy has been approved by the Managing Director of Carfax Education. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Managing Director.

**3. DEFINITION OF DATA PROTECTION TERMS**

**3. Definition of data protection terms**

**Definition of data protection terms**

This clause includes definitions of the most relevant data protection terms. The definitions are based on the definitions contained in [*section 1*](http://employment.practicallaw.com.lawdbs.lawcol.com/1-505-6034?pit=) of the DPA, but include additional plain English explanations of the various terms. For a more detailed description of the definitions contained in the DPA, see [*Practice note, Employer obligations under the Data Protection Act 1998 (www.practicallaw.com/3-200-2213)*](http://employment.practicallaw.com.lawdbs.lawcol.com/3-200-2213).

[Hide Note](http://employment.practicallaw.com.lawdbs.lawcol.com/9-379-8623?q=data+protection+policy#null)

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions,

religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

**4. DATA PROTECTION PRINCIPLES**Note: Data protection principles

**4. Data protection principles**

**Data protection principles**

This section includes a plain English description of the eight data protection principles set out in Part 1 of [*Schedule 1*](http://employment.practicallaw.com.lawdbs.lawcol.com/5-507-2777?pit=) to the DPA, together with a more detailed explanation of the meaning of some of those principles.

[Hide Note](http://employment.practicallaw.com.lawdbs.lawcol.com/9-379-8623?q=data+protection+policy#null)

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

1. Processed fairly and lawfully.
2. Processed for limited purposes and in an appropriate way.
3. Adequate, relevant and not excessive for the purpose.
4. Accurate.
5. Not kept longer than necessary for the purpose.
6. Processed in line with data subjects' rights.
7. Secure.
8. Not transferred to people or organisations situated in countries without adequate protection.

**5. FAIR AND LAWFUL PROCESSING**Note: Dealing with subject access requests

**5. Dealing with subject access requests**

**Dealing with subject access requests**

This section explains the procedure employees must follow when dealing with subject access requests. A data subject (including an employee of the company) has a right, on making a request to the data controller, to be informed whether personal data of which he is the data subject is being processed by or on behalf of that data controller ([*sections 7*](http://employment.practicallaw.com.lawdbs.lawcol.com/2-508-9307?pit=) *and* [*8*](http://employment.practicallaw.com.lawdbs.lawcol.com/8-508-9658?pit=)*, DPA*). If so, the data subject also has a right to:

* A description of the personal data held, the purposes for which it is being processed and the recipients or classes of recipients to whom the data may be disclosed.
* Any information available to the data controller as to the source of the data (subject to certain stated confidentiality and related protections for individual sources).

[Hide Note](http://employment.practicallaw.com.lawdbs.lawcol.com/9-379-8623?q=data+protection+policy#null)

5.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

**6. PROCESSING FOR LIMITED PURPOSES**

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

**7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING**

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

**8. ACCURATE DATA**

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

**9. TIMELY PROCESSING**

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

**10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS**

Data must be processed in line with data subjects' rights. Data subjects have a right to:

1. Request access to any data held about them by a data controller.
2. Prevent the processing of their data for direct-marketing purposes.
3. Ask to have inaccurate data amended.
4. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

**11. DATA SECURITY**

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

1. **Confidentiality** means that only people who are authorised to use the data can access it.
2. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
3. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

11.4 Security procedures include:

1. **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
2. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
3. **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
4. **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

**12. DEALING WITH SUBJECT ACCESS REQUESTS**

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their Managing Director.

**13. PROVIDING INFORMATION OVER THE TELEPHONE**

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

1. Check the caller's identity to make sure that information is only given to a person who is entitled to it.
2. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
3. Refer to their Managing Director.

**14. DATA PROTECTION REGISTRATION**

Organisation name: **Carfax Tutorial Establishment Limited**

Registration reference:**ZA210372**

**15. MONITORING AND REVIEW OF THE POLICY**Note: Monitoring and review of the policy

**14. Monitoring and review of the policy**

**Monitoring and review of the policy**

Any commitments to reviewing and monitoring a policy, and to offering and providing training to staff, should be honoured.

[Hide Note](http://employment.practicallaw.com.lawdbs.lawcol.com/9-379-8623?q=data+protection+policy#null)

15.1 This policy is reviewed regularly by our administrative staff in consultation with the Managing Directors.

15.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.