

This is a sample – not the full document

**Buy the full document in Word format.
Select from the following options:**

Individual Document

<http://www.compactlaw.co.uk/data-protection-policy.html>

Employers Pack

<http://www.compactlaw.co.uk/employers-pack.html>

Workplace Pack

<http://www.compactlaw.co.uk/workplace-pack.html>

DATA PROTECTION POLICY

This policy document applies to your employment at *[Insert organisation name and address]* ("the Organisation") and all other Organisation sites that you may be asked to work at from time to time.

1. Data Protection Principles

The Organisation complies with the Data Protection Act 1998 and the principles of the Act, your personal data will be:

1. Fairly and lawfully processed.
2. Processed for limited purposes and not in any way incompatible with those purposes.
3. Adequate, relevant and will not be excessive.
4. Accurate.
5. Not kept for longer than necessary
6. Processed in accordance with your individual rights.
7. Secure.
8. Not transferred to countries without adequate data protection.

2. Your Agreement

As part of your employment within the Organisation you agree to the collection and storage of your personal data within the scope of the Data Protection Act 1998.

3. Your Personal Data

3.1 The Organisation only holds personal data directly relevant to your employment. This data is collected as and when required from your first employment application form and from your continuing employment within the Organisation, such information includes, but is not limited to:

- i)** Third-party employment references.
- ii)** Employment reports or assessments, including performance reviews.
- iii)** Disciplinary details, including informal or formal warnings.
- iv)** Grievance procedures and outcomes.
- v)** Salary reviews, benefits records and expenses claims.
- vi)** Health records.

3.2 This information is only collected to assist our personnel department in the smooth running of the Organisation and to ensure that the Organisation complies with other statutory responsibilities such as equal opportunities employment.

3.3 Your personal data may be disclosed within the Organisation to those within the personnel department and management, including your immediate manager. Your personal data will not be disclosed to your peers or any other employees that do not require access to the data in order to carry out their own roles within the Organisation.

4. Maintaining Records

The Organisation will take all reasonable steps to ensure that personal data held by the Organisation is accurate and kept up to date. To ensure accuracy the Organisation will ask employees every 12 months to check that their personal information held by the Organisation is correct. As an employee you should always contact the personnel department should your personal information change for any reason, for example a change of surname, home address or telephone number. Out of date information or information that is no longer required will be deleted by the Organisation on a regular basis.

5. Sickness & Health Records

For day-to-day management the Organisation needs to keep records relating to the personal sickness and health records of each employee. Such personal data will record any periods of sickness or health matters, detailing the length and nature of the issue and the outcome. These records will be used to assess the health and welfare of employees and to highlight any issues that may require further investigation. Such data will only be disclosed to management and will not be disclosed to fellow employees, (except those employees within the personnel department who process such data). If for any reason you do not wish your health records to be kept please contact [*Insert manager's name*], [*Insert manager's position*].

6. Security of Data

6.1 The Organisation is committed to the secure storage and where undertaken the secure transmission of employees' personal data. Only management and employees within the personnel department have access to such data. All such data is protected by physical security, such as locks and technical security, such as usernames and passwords to access computer records and data. Such data is only disclosed on a "need to know" basis. To further ensure the security of such records the Organisation reserves the right to monitor and keep detailed log file and computer data analysis of all accesses to employees' personal data. The Organisation also reserves the right to vet all employees who have access to such data in the course of their normal employment within the Organisation.

6.2 If as an employee you have legitimate access to personal data and you pass or transmit the data within the Organisation to another party or parties who in turn have the right to see such data, the following rules apply:

- 1.** If the data is transmitted by email it must be sent in an encrypted form.
- 2.** If the data is transmitted via a network it must be done using a secure network. Wherever possible such data should not be sent via a wireless network where the risk of interception is greater.
- 3.** Such data should not be kept within the email program on your PC after it has been sent or received. The data must be removed from the body of the email message or deleted from any temporary folders if sent as an attachment. Care should be taken at all times not to delete the original data source.
- 4.** If the data is to be faxed ensure that the intended recipient knows in advance that the data is coming via fax and that they are standing by the fax machine to receive the data. Ensure that the fax number is correct. You should also confirm safe receipt of the data by the recipient.
- 5.** If data is to be passed in hard copy form it should be handed to the recipient personally, the recipient should ensure that the data is stored in a locked drawer or cabinet.

6.3 Parties with legitimate access to such data should not use third parties without the authority to view the data to send or receive the data on their behalf.

6.4 All employees are reminded that unauthorised attempts to gain access to such data or accessing such data is a disciplinary offence and in certain situations may constitute gross misconduct leading to summary dismissal. Such breaches may also constitute a criminal offence under the Data Protection Act 1998.

7. External Data Processing

Where the Organisation uses third parties to process data and provide services or administer schemes around such data the Organisation will take reasonable steps to ensure that such third parties have in place their own data protection policies.

Sample document – the remaining are clause headings only
Full document contains all clauses

8. Benefits Schemes

9. Equal Opportunities Monitoring

10. Employee Reviews & Appraisals

11. Data Transfers Outside The European Economic Area

12. Data Access & Disclosure

13. References

14. External Disclosure Requests

15. Other Disclosures

16. Trade Unions

17. Employee Monitoring

18. CCTV Monitoring

19. Medical Testing

20. Retention of Employee Records

21. Criminal Liability

22. Date of Implementation

23. Questions

24. Alteration of these Guidelines

(c) <http://www.compactlaw.co.uk>

<http://www.compactlaw.co.uk/data-protection-policy.html>