

DATA PROTECTION POLICY

In the course of work, an employee or contractor may come into contact with, or use confidential information about other employees or contractors, clients, customers and suppliers, for example, their names and home addresses. The **Data Protection Act 1998** contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer, but also certain manual records containing personal data, for example, employees' personnel files forming part of a structured filing system. If an employee or contractor is in any doubt about what he/she can or cannot disclose and to whom, they should not disclose the personal information until he/she has sought further advice from the Operations Director, who is in charge of data protection compliance. An employee or contractors should be aware that he/she could be criminally liable if he/she knowingly or recklessly discloses personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence. If an employee/associates accesses another employee's or contractor's personnel records without authority, this constitutes a gross misconduct offence and could lead to a summary dismissal/revocation of contract.

Although this policy is specific to employees, its content equally apply to contractors and to learners registered with The Business School Ltd.

The Data Protection Principles

There are eight data protection principles that are central to the Act. We and all our employees, associates, learners and contractors must comply with these principles at all times in our information-handling practices. In brief, the principles say that personal data must be:

- Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that an employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of an employee, and consists of information relating to: race or ethnic origin; political opinions and trade union membership; religious or other beliefs; physical or mental health or condition; sexual life; criminal offences, both committed and alleged.
- Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.
- Adequate, relevant and not excessive. We will review personnel files on a regular basis to ensure they do not contain a backlog of out-of-date information, and to check that there is sound business reason requiring information to continue to be held.
- Accurate and kept up-to-date. If an employee's personal information changes, for example, he/she changes address or he/she gets married and changes their surname, he/she must inform the line manager as soon as practicable so that our records can be

updated. We cannot be held responsible for any errors unless an employee has notified us of the relevant change.

- Kept for only as long as is necessary. We will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data that we decide we do not need to hold for a period of time, will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.
- Processed in accordance with the rights of employees under the Act.
- Stored with adequate security. Technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Hard copy personnel files are confidential and are stored in locked filing cabinets. Only authorised employees are permitted to have access to these files. Files must not be removed from their normal place of storage without good reason. Personal data stored on diskettes or other removable media must be kept in locked filing cabinets. Personal data held on computer must be stored confidentially by means of password protection, encryption or coding, and again only authorised employees are permitted to have access to that data. We have network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.
- Only transferred to a country or territory outside the European Economic Area if that country ensures an adequate level of protection for the processing of personal data.

Employees' Consent to Personal Information being Held

We hold personal data about employees and their consent to us processing employees' personal data is a condition of their contract of employment. Therefore, by agreeing to their contract of employment, the employees also agree to their personal data being held and processed. We also hold limited sensitive personal data about our employees, and by signing the contract of employment, employees give their explicit consent to us holding and processing that data, for example, sickness absence records, health needs and equal opportunities monitoring data.

Employees' Right to Access Personal Information

Under the provisions of the Act, employees have the right, on request, to receive a copy of the personal data that we hold about them, including their personnel file, to the extent that it forms part of a relevant filing system, and to demand that any inaccurate data be corrected or removed. Employees have the right on request:

- To be told by us whether, and for what purpose, personal data about an employee is being processed
- To be given a description of the personal data and the recipients to whom it may be disclosed

-
- To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the personal data
 - To be informed of the logic involved in computerised decision making.

Upon request, we will provide an employee with a written statement regarding the personal data held about him/her. We reserve the right to charge employees a fee of up to £10.00 per request. To make a request, please apply to the Operations Director who is in charge of data protection compliance.

If an employee wishes to make a complaint that these rules are not being followed in respect of personal data we hold about him/her, he/she should raise the matter with the Operations Director who is in charge of data protection compliance. If the matter is not resolved to his/her satisfaction, it may then be raised as a formal grievance.

Employees' Obligations in Relation to Personal Information

Employees should ensure that they comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party, unless the data subject has given his or her explicit consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- Only transmit personal information between locations by fax or email if a secure network is in place, for example, a confidential fax machine or encrypted email.
- If an employee receives a request for personal information about another employee, he/she should forward this to the Operations Director, who will be responsible for dealing with such requests.
- Ensure any personal data employees hold is kept securely, either in a locked filing cabinet or if computerised, that it is password protected.
- Compliance with the Act is the responsibility of the employees. If employees have any questions or concerns about the interpretation of these rules, they should take this up with the Director who is in charge of data protection compliance.

We are registered with the Information Commissioner's Office as follows:

Registration Reference A8147826

We process information to enable us to provide education and training to our customers and clients; to promote our services, to maintain our own accounts and records and to support and manage our employees.