Data Protection, Document Storage & Retention Policy

1 Overview

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, Customers, suppliers and subcontractors we recognise the need to treat it in an appropriate and lawful manner.

The types of information that may be required to handle includes details of current, past and prospective employees, supplier's information, customers personal details and others that we communicate with. The information, which may be held on paper or on a computer via our Data Base, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) and other regulations. The Act imposes restrictions on how we may use that information. This also meets the requirements of GDPR.

If you consider that our provisions for complying with the Act have not been followed in respect of personal data about yourself or others you should raise the matter with your Line Manager and Boss Training's Operations Manager.

2 Definition of Data Protection Terms

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

b) Data subjects for the purpose of this policy, includes 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.

c) 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).

d) 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.

e) 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.

f) 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.

g) 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.

h) 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.

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

a) Processed fairly and lawfully.
b) Processed for limited purposes and in an appropriate way.
c) Adequate, relevant and not excessive for the purpose.
e) Accurate.
f) Not kept longer than necessary for the purpose.
g) Processed in line with data subjects' rights.
h) Secure.
i) Not transferred to people or organisations situated in countries without adequate protection.

4 Fair and Lawful Processing
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 (in this case it is us), 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.
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.

5 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.

6 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.

7 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.

8 Timely Processing/ Document retention
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.
All Financial data will be retained for a period of 6 years.

Course data will be retained for a period of 6 years, unless under a separate agreement with an accrediting body or a customer. i.e. Morson Human Resources have requested that we store Data for 7 Years.
Any Investigation of Malpractice or into Reasonable Adjustment, safeguarding or Equality stall be retained for 7 years.

9 Processing in Line with Data Subject's Rights
Data must be processed in line with data subjects' rights. Data subjects have a right to:

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

10 Data Security
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. 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 they put in place adequate measures themself.
Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

a) Confidentiality means that only people who are authorised to use the data can access it.
b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
c) 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 Security procedures include:
a) Entry controls, any stranger seen in entry-controlled areas should be reported. Access to data current or archived is provided to only those individuals who, in the course of performing their responsibilities and functions must use the specified data. No data is shared with any third party and should never be removed from the office, other than organisations outlined in section 15 "Accrediting or Registered Bodies".
b) Secure areas, 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.) All customer/delegate/supplier details are stored on a secure database. This is password protected, as are all office PC’s. All data is backed up to the server automatically on a daily basis. A full server backup to external hard drive takes place weekly. Weekly backups are securely stored off-site
c) All data on the network is protected by ESET end point security anti-virus software that runs on servers and workstations, and is updated automatically with on-line downloads from the website. This includes alerts whenever a virus is detected.

d) Hard copies of invoices and delegate question papers are stored in secure cupboards at head office and all archived documents are stored in locked cupboards and shredded after 10 years storage. However, individual coarse information will be destroyed after 3 years, but the Company will keep hold of a course register which will details of which candidates passed which course and date.
e) Credit card payments taken via the World Pay system are processed and receipts sent directly by email and copies stored securely within the system. No hard copies of card payments are ever made (if card details are ever recorded by an employee this is seen as gross misconduct, this will be immediately enforced in line with the disciplinary procedure)
f) Methods of disposal. Whether hard copy or electronic should be destroyed in a secure manner, preserving the confidentiality of all personal data. All hard copy data must be disposed of in the confidential waste bins which are located in the admin office. Under no circumstances should confidential or personal data be put into normal waste bins.
g) We will maintain records of the secure destruction of all waste which is put into the confidential waste. We will ensure that all electronic data is securely destroyed in a way which cannot be restored. We will also be responsible for ensuring that any electronic equipment is securely wiped, and where appropriate securely disposed of, when it is no longer required by the business.
Suspending the destruction date If a claim, audit, investigation, subpoena, or litigation has been asserted or filed by or against us, or is reasonably foreseeable, we have an obligation to retain all relevant records, including those that otherwise would be scheduled for destruction under the records retention schedule.
h) 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. All staff adheres to a ‘clear desk’ and ‘clear screen’ policy. All PC’s are switched off when not in use.
Boss Training Ltd registered with the ICO under registration reference: Z2087267

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. If you receive a written request you should forward it to the Operations & Compliance Manager immediately.

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:
a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.
b) 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.

Refer to the Operations Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

14 CCTV
We have a CCTV System in place that also contains enables Audio recording at our Halifax Training Centre the purpose of the CCTV Audio system is to ensure the invigilation process is adhered to in the Courses we provide. We will not use the system for any incompatible purposes and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

We have registered as a controller with to the Information Commissioner's Office (ICO). The annual renewal date is 2nd February.

The individual who is responsible for the operation of the system is Stacy Stanger.

We will regularly review our decision to use a surveillance system.

We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018. That, the individual will have given clear consent for you to process their personal data for a specific purpose.

Our system produces clear images which we can easily disclose to authorised third parties. For example, CITB.

We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.

There are visible signs showing that CCTV is in operation.

We will securely store images from this system for a period of 40 working days and only a limited number of authorised individuals may have access to them.

Our organisation knows how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted. If unsure the controller knows to seek advice and guidance from the Information Commissioner's Office (ICO) as soon as a request is made.

15 Accrediting or Registered Bodies.

All courses that are provided or approved by an external accrediting or registered body, such as, but not limited to PASMA, IPAF, NPORS, UKATA, CITB, NOCN & Qualsafe.
Such courses are either provided by the accrediting/registered body or are regularly reviewed by them. Boss Training will allow personal data to be transferred to accrediting or registered bodies for the following purposes:

a) To undertake administration in relation to the learner's registered qualification.
b) To provide centres with a certificate for the learner.
c) To contact the learner directly regarding assessment or quality assurance purposes for the qualification they are registered on, or for the purpose of investigations into suspected malpractice. This includes the learner's personal telephone number.
d) To disclose to accrediting or registered bodies regulators or sector skills bodies where so required.
e) To administer requests for Reasonable Adjustments and Special Considerations.
f) To carry out statistical analysis and monitor equal opportunities (anonymised).

16 GDPR OFFICER

If You Have any queries regarding GDPR Please contact our GDPR Officer Matthew Lloyd matthew@bosstraining.co.uk.