# DATA PROTECTION/GDPR/PRIVACY POLICY

## Policy Statement

Holt Green Training Ltd is committed to a policy of protecting the rights and privacy of individuals (includes learners, staff and others) in accordance with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR)

The company needs to process certain information about its staff, learners and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and learners of the company. Any breach of the Data Protection Act 1998, the GDPR or the Training Company Data Protection Policy is considered to be an offence and in that event, HGT disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the company, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

**Background to the Data Protection Act 2018**

The Data Protection Act 2018 replaced the Data Protection Act 1984, and the General Data Protection Regulation, which replaced the 1995 Data Protection Directive, came into force in March 2018.

The purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Article 5 of the GDPR requires that personal data shall be:

“processed lawfully, fairly and in a transparent manner in relation to individuals; collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

**Definitions**

*Personal Data*

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, and id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

*Sensitive Data*

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

*Data Controller*

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

*Data Subject*

Any living individual who is the subject of personal data held by an organisation.

*Processing*

Any operation related to organisation, retrieval, disclosure and deletion of data and includes Obtaining and recording data accessing, altering, adding to, merging or deleting data.

*Third Party*

Any individual/organisation other than the data subject, the data controller (Training Company) or its agents.

*Relevant Filing System*

Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

**Responsibilities of the Data Protection Act**

- The company as a body corporate is the data controller under the new Act.
- Compliance with data protection legislation is the responsibility of all members of the company who process personal information.
- Members of the company are responsible for ensuring that any personal data supplied to the company are accurate and up-to-date.
-

**Data Protection Principles**

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully.

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

Information which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date.

Data, kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume accurate. It is the responsibility of individuals to ensure that data held by the Training Company is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken, as an indication that the data contained therein is accurate. Individuals should notify the Training Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Training Company to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Personal data shall be kept only for as long as necessary. (See Section 12 on Retention and Disposal of Data)

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act. (See Section 7 on Data Subjects Rights)

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. (See Section 9 on Security of Data)

8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of the Training Company should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

**Data Subject Rights**

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

**Consent**

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The company understands "consent"

to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord.

Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the company (e.g. when a student signs a registration form or when a new member of staff signs a contract of employment). Any company forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the company is in any doubt about these matters, they should consult the Operations Manager

**Security of Data**

All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

All personal data should be accessible only to those who need to use it. You should form a judgment based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and learners who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and learners should take particular care when processing personal data at home or in other locations outside the Training Centre.

**Rights of Access to Data**

Members of the company have the right to access any personal data, which are held by the Training Company in electronic format and manual records, which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the company about that person. Any individual who wishes to exercise this right should apply in writing to the Operations Manager. The company reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. In order to respond efficiently to subject access requests the company needs to have in place appropriate records management practices.

**Disclosure of Data**

The company must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All staff and learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular

function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of company business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the company concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. The individual has given their consent (e.g. a student/member of staff has consented to the company corresponding with a named third party);
2. Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other company employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. Where the institution is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring);
4. Where disclosure of data is required for the performance of a contract (e.g. informing a student's LEA or sponsor of course changes/withdrawal etc.).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security*;
- Prevention or detection of crime including the apprehension or prosecution of offenders*;
- Assessment or collection of tax duty*;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- To prevent serious harm to a third party;
- To protect the vital interests of the individual, this refers to life and death situations.
- Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the company, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the company may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the company may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer;
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Training Company" to avoid confirming their membership of, their presence in or their absence from the institution.

**Retention and Disposal of Data**

The Training Company discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and learners. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

**Learners**

In general, electronic student records containing information about individual learners are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

Departments should regularly review the personal files of individual learners in accordance with the company's Records Retention Schedule.

**Staff**

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc. will be retained for the statutory time period (between 3 and 6 years).

Departments should regularly review the personal files of individual staff members in accordance with the company's Records Retention Schedule (Appendix VII).

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

**Disposal of Records**

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

**Publication of Company Information**

It is recognised that there might be occasions when a member of staff, a student, or other member of the company, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the company should comply with the request and ensure that appropriate action is taken.

**Direct Marketing**

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).