Data Protection and Confidentiality Policy

Last reviewed: September 2022

Signature: *J Sharpe* (Principal)

Signature: *H Sapsford* (Operations Manager)

Policy overview

It is the Company's (Dv8 Education & Training CIC) policy to take all necessary steps to ensure that personal data held about its employees, learners, customers, suppliers and all other individuals is processed fairly and lawfully. The Company will take all reasonable steps to implement this policy. The Company will implement and comply with the seven key principles of the General Data Protection Regulation (GDPR) ("the Regulation") which promotes good conduct in relation to processing personal information. These principles are:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

- 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 ('purpose limitation');

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- 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 ('accuracy');

- 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 ('storage limitation');

- 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 ('integrity and confidentiality').

The Company will use all data in accordance with the rights given to individuals' under the General Date Protection Regulation, and will ensure that it allows individuals' to exercise their rights. This regulation enables individuals to have control over how their data is collected, stored and what is done with it.

The different types of right are as follows;

- Subject Access Requests
    - Individuals have the right under the GDPR to ask a College to confirm what personal data they hold in relation to them and provide them with the data. The timescale for providing it is one month (with a possible extension if it is a complex request).

    - Where the request is complex and it will take more than one month the reason for delay will be explained in writing to the data subject making the request.

- Right of Erasure (Right to be Forgotten)
    - This is a limited right for individuals to request the erasure of personal data concerning them where;
        - The use of the personal data is no longer necessary;
        - Their consent is withdrawn and there is no other legal ground for the processing;
        - The individual objects to the processing and there are no overriding legitimate grounds for the processing;
        - The personal data has been unlawfully processed;
        - The personal data has to be erased for compliance with a legal obligation
- Right of Data Portability
    - An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where;
        - The processing is based on consent or on a contract; and
        - The processing is carried out by automated means
    - This right isn't the same as subject access and is intended to give individuals a subset of their data.
- The Right of Rectification and Restriction
    - Individuals are also given the right to request that any personal data is rectified if inaccurate and to have use of their personal data restricted to particular purposes in certain circumstances.
- Automated Decision Making and Profiling
    - Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.
        - Automated Decision Making happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects;
        - Profiling happens where the College automatically uses personal data to evaluate certain things about an Individual.
        - The Company does not currently carry out automated decision making or profiling in relation to it's employees or learners. Should this ever change The Company will consult fully with our DPO and follow all Data Protection Laws.

<u>Employee Obligations</u>

Employees have a duty to follow the Company's rules and procedures and to co-operate with the Company to ensure this policy is effective. Disciplinary action may be taken against any member of

staff who fails to comply with these rules and procedures.
All employees must complete a Data Protection Consent form to be found in the Dv8 Starter Forms.

The Company has a responsibility to ensure that personal data dealt with in the course of its business is handled in accordance with statutory requirements and reasonable steps will be taken by all concerned to ensure this duty is observed.

The Company will take such measures as may be necessary to ensure the training of all relevant staff in matters pertaining to data protection and to provide any necessary information.
The person having overall responsibility for data protection will be the Prinicpal.
Each member of staff will have immediate responsibility for data protection matters in his / her own area of work. Any queries should be raised with their respective Line Manager.

Data Protection Rules and Procedures

Data protection is a responsibility shared by all employees of the Company. Staff must familiarise themselves with and observe at all times these Rules and Procedures relating to data protection, the Data Protection Policy Statement and any additional instructions which may be issued from time to time.

Each member of staff will have responsibility for data protection matters in his / her own immediate area of work, but in addition, many employees carrying out their normal duties may be required to process personal data within the meaning of the DPA 1998; for example, information about customers, suppliers or fellow staff members.

Staff who have any queries, comments or suggestions in relation to data protection should contact their Line Manager. Service users should contact a member of the Senior Management Team.

Personal data should only be used for the purpose or purposes advised to the individual and not for any ancillary purpose. For example, if an individual such as a supplier or customer was informed that his / her data would only be used for marketing purposes, then such data cannot be used for any purpose other than marketing.

Informed consent must be sought before any individual on a training course is photographed, recorded or videoed. This informed consent should be recorded via the Company's Data Protection Consent Form.

Personal data held about an individual should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is held. All opinions and / or statements of fact recorded about the individual must be accurate and relevant to the purpose or purposes for which the personal data is held.

Personal data held about an individual must be kept up-to-date and accurate, and all staff are required to notify their Line Manager of changes in their circumstances so that accurate, up-to-date records can be maintained. Learners are required to notify the Centre Offices of any changes, in line with their Enrolment and Learning Agreement.
If the individual staff member or learner, as the case may be, withholds his / her consent or if his /

her consent is not provided, then immediate reference should be made to the Senior Management Team where the request will be processed within one month of receipt.

Learner personal details and basic progress information may be shared with statutory bodies within Integrated Support Services or other local authority jurisdiction, but only if such sharing is justified in the learner's interest and results in the management of progression or the reduction of risk.

Security of Data

All personal data held by the Company is to be treated as strictly confidential.
Personal data must not be disclosed to anyone outside the Company unless the individual concerned has consented to such disclosure, or the Managing Director has given a specific instruction to do so within lawful processing.

Personal data must not be disclosed to any unauthorised employees. The Senior LeadershipTeam will establish and control personal data access.

User passwords will be issued to relevant employees who deal with computerised personal data. Such user passwords are not to be disclosed to any third party or unauthorised employee and these should always be used in connection with any personal employment related documentation. In relation to all employee related HR documentation this will be stored initially by the centre manager for maintenance with only the direct line manager of that individual and the HR officer having access.
Where access is sought from another staff member (other than the direct line manager) written consent should be gathered from that employee.

Standard documentation about students is shared with funders however where sensitive information is recorded (this could be in student support session notes or on the students notes system) this will be done on a need to know only basis..

Personal data MUST be kept in a locked cabinet/cupboard at all times or in password encrypted digital files. Individuals will have a right, on written request, to obtain a copy of such personal data relating to him / her held by the Company as is required under the General Data Protection Regulation. All requests by individuals for information about personal data the Company holds about them must be referred, immediately on receipt, to their Line Manager/ Centre Offices who will co-ordinate the response to the relevant individual. The Company reserves the right to charge a fee for this service.
The Principal will determine the level of fee to be charged.

Personal data collected on learners will be accessed only by authorised current staff and will be kept securely, whether on paper or electronically. This information will be held centrally for no more than five years, unless otherwise instructed to do so by a regional, national or contracting authority to whom the Company is directly accountable.

Personal data collected on prospective learners, who never formally enroll on any Dv8 programme, will be held centrally for no more than one year.

Data Breach

The Company takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of personal data. If this happens there will be a personal data breach and Company Personnel must comply with Data Protection Laws set out by GDPR. A personal data breach can be defined very broadly and is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data.

The main types of data breach are;

- Confidentiality Breach
    - where there is an unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing personal data stored on a lost laptop, phone or other device, people "blagging" access to personal data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- Availability Breach
    - where there is an accidental or unauthorised loss of access to, or destruction of, personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from back up, or loss of an encryption key;
- Integrity Breach
    - where there is an unauthorised or accidental alteration of personal

data. All breaches will be dealt with urgently and in line with Data Protection Laws.

Contractors

If the Company appoints a contractor who is a Processor of the Companies personal data, Data Protection Laws require that the Company only appoints them where the Company has carried out sufficient due diligence and only where the Company has appropriate contracts in place. The Company will only use processors who comply with the GDPR and the rights of the individual. All contractual processors will be audited annually, alongside our general data protection audit.

Confidentiality

The term 'confidential information' is defined as personal information that will only be shared with other appropriate people who need to know. The "test" for the "need to know" is whether the interests of the individual or others will be adversely affected if the information remains unshared. At Dv8 we use MyConcern to keep young people 'safe' and to ensure we are following best practice in regard to our duty of care responsibilities. In these cases, we will only share information within the Dv8 staff team (e.g staff working directly with that young person) on a need to know basis and not to any external agencies.

However, if information given suggests that any young person or vulnerable adult is at serious risk of harm or is putting others at risk, then this information can be shared with other staff, workplaces

or other relevant agencies without consent. We will always inform the young person that we will be passing their disclosure and information on in these incidences to keep young people informed of who we have shared their information with and how.

In incidences where sensitive discussions are taking place between staff and students, Dv8 will ensure that this happens in a safe, confidential space at Dv8 like the one-to-one room. No conversations of this nature will take place in any public areas.

Data Protection Officer: [redacted]