PROVEK
DATA PROTECTION & PRIVACY POLICY

provek
enabling change

Document Control

Document version history

Document version	Date issued	Comments
V1-0	16/02/2021	

Next review date

February 2022

Document distribution

File

All Provek staff

Website

Contact Details

Provek Ltd.

12 Thatcham Business Village

Colthrop Way

Thatcham

RG19 4LW

Tel 01635 524610

Fax 01635 524620

Email enquiries@provek.co.uk

Web www.provek.co.uk

Contents

Provek data protection & privacy policy

Purpose

Everyone has rights regarding the way in which their personal data in handled. Provek Limited is an apprenticeship training provider, specialising in adult technical and vocational education. During our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Provek collects, evaluates and stores a range of personal information and records of learning. This personal data is processed to facilitate delegate learning. Examples of data collected includes:

- Online satisfaction/feedback surveys
- Expression of Interest forms
- Assessment of current knowledge & experience forms (PMA)
- Commitment Statements

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

This guidance is to be read in conjunction with the following Provek policies:

- Provek IT Security policy
- Provek Complaints and Appeals policy

Scope

The types of personal data that Provek Limited (We) may be required to handle include information about current, past and prospective customers, learners, employees and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act), the General Data Protection Regulations (GDPR) and other regulations.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy has been approved by the Senior Management Team of Provek Limited and sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

Definition of data protection terms

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

Data subjects for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

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 (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controllers are the people who or organisations which determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on Provek Limited's behalf.

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.

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. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Data protection principles

Anyone processing personal data must comply with the seven enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose (data minimisation).
- Accurate.
- Not kept longer than necessary for the purpose (storage limitation).
- Secure (integrity and confidentiality).
- Processed in a compliant manner, with those processing such data to be responsible for complying with the GDPR and demonstrating their compliance (accountability).

Fair and lawful processing

The Act is not intended 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.

For personal data to be processed lawfully, they must be processed based on one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers during our business, we will ensure that those requirements are met.

Processing for limited purposes

During our business, we may collect and process your personal date. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data as required for business purposes or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Such personal data is processed and securely stored on our virtual learning environment, (Bud) and Provek's IT systems, accessible by only Provek staff.

Notifying data subjects

If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data.
- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- The means, if any, with which data subjects can limit our use and disclosure of their personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we process that we are the data controller regarding that data.

Adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Processing in line with data subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

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

Data security

We will process all personal data we hold in accordance with our Data Security Policy **OR** take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data].

We will 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 will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **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 the Provek's central computer system instead of individual PCs.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure 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.)
- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- **Equipment.** Data users must 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.

Transferring personal data to a country outside the EEA

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Disclosure and sharing of personal information

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may also disclose personal data we hold to third parties:

- If we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
- If all or substantially all our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

If we are under a duty to disclose or share a data subject's personal data to comply with any legal obligation, or to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We may also share personal data we hold with selected third parties for the purposes set out in this policy.

Dealing with subject access requests

Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it the Operations Director immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Our employees will refer a request to their line manager or the Operations Director for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

Timely processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Data Retention Policy

This sets out the guidelines on what data will be archived, how long it will be kept, what happens to the data at the end of the retention period and other factors concerning the retention of data held by Provek relating to its staff, students, clients and employers.

The Data Protection Act ('the Act') applies to most personnel records, whether held in paper or computerised format. The Act requires that personal information in a record should be kept for no longer than necessary for a particular purpose. Computerised systems are covered by the law, as are certain manual systems.

Subject to certain exceptions (Schedule 7 of the Act) employees have the right to access their records and the employer is under an obligation to ensure that data is accurate.

Data includes information that is in manual records, i.e. paper or non-computer form.

Retention of records

The Data Protection Act does not specify what a 'necessary' period should be for information and each case is considered on its own merits.

For example, financial institutions may have to keep information for up to six months in accordance with the Financial Services Authority regulations, but a sole trader may not need to keep information for longer than a month.

Therefore, as there is no specific period given in the Act, it is for the employer to set retention periods.

Provek will undertake to ensure that:

- personal information is not kept for longer than necessary
- It is not deleted where there is a real business need to retain it.

Legal responsibilities

Provek is registered with the Information Commissioner for processing information and is required to comply with the Data Protection Act and undertakes to process personal information in accordance with the eight principles of the Act and to answer Subject Access Requests received from individuals.

Provek also undertakes to consider that information should not be retained simply on the basis that it might come in useful and will:

- Establish how often particular categories of information are accessed after e.g. 5 years
- Adopt a 'risk analysis' approach to retention and consider what would be the consequences for the business where information that is rarely accessed is no longer available.
- Base any decision to retain a record on the principle of proportionality- i.e. many records should not be retained for a long period in case one of them wishes to question an aspect of their employment.
- Treat items of information individually or in logical groupings and not just retain all the information in a record because it is necessary to retain some of it.

Therefore, records must not be kept beyond the standard retention time unless there is a business justification for doing so.

Computer records, when deleted, must be removed from the system, and computer equipment must not be sold on unless the employer is certain that any employment records have been removed.

Provek will check periodically whether all information is needed, for example by carrying out an audit.

If it is possible to satisfy the business' needs without retaining information in a form that can identify people, then Provek will.

If Provek is under a legal obligation to keep information for a specific period, e.g. for accounting purposes, the Data Protection Act will not prevent them from doing so.

Access to personal information

- The Data Protection Act 1998 gives individuals the right to access personal information that is processed about them.
- To obtain access to personal information, an individual must send either a written or electronic request to Provek (a subject access request (SAR)).
- Provek may at its discretion charge up to £10 for providing the information and will respond to a SAR no later than 40 days after receiving it.

Personnel data retention periods

- Personnel security records will be kept as separate annual sub-sets of personal files (and so can be destroyed on a rolling basis).
- Medical records will be filed as a separate sub-set of individual personal files to allow for separate retention.
- Details of retention periods for personnel date are set out in the table below.

Statutory retention periods

Type of Record	Retention Period	Resp
Statutory Retention Period		
Workplace accidents	Three years after date of last entry.	HR
Payroll	Three years after the end of the tax year they relate to	Finance
Statutory maternity, adoption and paternity pay	Three years after the end of the tax year they relate to	Finance
Statutory sick pay	Three years after the end of the tax year they relate to	Finance
Working time	Two years from date on which they were made	HR
National minimum wage	Three years after the end of the pay reference period following the one that the records cover	HR
Retirement benefits schemes - notifiable events, e.g. relating to incapacity	Six years from the end of the scheme year in which the event took place	Finance
Accounting Records	3 years	Finance
Other Records		
Application forms/interview notes for unsuccessful candidates	One year	HR
Health and safety consultations	Permanently	HR
Parental leave	Five years from birth/adoption, or until child is 18 if disabled	HR
Pensioners' records	12 years after benefit ceases	Finance
Disciplinary, working time and training	Six years after employment ceases	HR
Redundancy details	Six years from date of redundancy	Finance
Information on senior executives	Permanently for historical purposes	HR
Trade union agreements	Ten years after ceasing to be effective	HR
Minutes of trustee/work council meetings	Permanently	HR
Documents proving the right to work in the UK	Two years after employment ceases	HR

Complaints

Should data subjects have any complaints, they are advised to refer to Provek's Complaints and Appeals Policy and follow the procedure accordingly.