Perthshire Wellbeing Project Data Protection Policy.

1. Scope

This policy describes how personal data is collected, handled and stored to meet Perthshire Wellbeing Project data protection standards and to comply with the law.

The UK General Data Protection Regulation (UK) GDPR 2018 and Data Protection Act 2018 applies to every business that collects, stores and uses personal data relating to customers, staff or other individuals.

(UK) GDPR and DPA (2018) applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. (UK) GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

1.1. The policy applies to:

- The training facilitators of Perthshire Wellbeing Project
- Other people

1.2. It applies to all data that the company collects and holds relating to: All individuals and or customers

- Postal addresses
- addresses
- Telephone numbers
- IP addresses, cookies, electronic data
- Plus, any other information relating to Email individuals, and or customers

2. Responsibilities

3. Perthshire Wellbeing Project needs to gather and use certain information from customers, suppliers, businesses, employers, instructors and other people the company has a relationship with or may need to contact. Everyone who works for or with Perthshire Wellbeing Project. has some responsibility for ensuring data is collected, stored and handled appropriately.

3.1. Perthshire Wellbeing Project data protection manager

3.2. Gordon Stronach is responsible for:

- Awareness of data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies, in line with schedule
- Arrange data protection training and advice for employees
- Handling data protection questions and dealing with customer requests
- Checking for sensitive data in any contracts or agreements with third parties
- Ensuring all systems, services and equipment meet acceptable security standards
- Ensuring safe and secure storage of training or assessment materials
- Achievement data is retained for the purposes of reporting to the regulatory authorities as required
- Preform regular hardware and software checks and scans
- Evaluating any third-party services for the purpose of storing or processing data
- Approve any data protection statements attached to emails, letters, communication
- Provide guidance to use BCC box when sending emails to groups unless absolutely certain that permission was given for individual details to be made available to others
- Ensure marketing initiatives comply with the data protection principles
- Ensure forms have appropriate data protection notifications on them

4. (UK) GDPR/DPA and the law

Under General Data Protection Regulation ((UK) GDPR) and DPA (2018) organisations including Perthshire Wellbeing Project must collect, handle and store personal data. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

“Personal data” is defined in both the Directive and the (UK) GDPR as any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Perthshire Wellbeing Project makes no distinction between personal data about individuals in their private, public or work roles – the person is the person. Online identifiers including IP address, cookies and so forth are also regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject.

“Personal Data Breach" is defined in the (UK) GDPR as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed”. Data breaches will be reported to ICO Commission within 72hrs

Perthshire Wellbeing Project only collects personal data for specified purposes and does not use it for other ‘incompatible’ purposes. Example: Individuals details are not used for marketing purposes if originally collected for an entirely different purpose.

Perthshire Wellbeing Project is registered with the Information Commissioner's Office (ICO) to process personal data. As a registered body, we determine the purposes for which, and the manner in which, personal data is to be processed.

The Scottish Information Commissioner and the UK Information Commissioner's Office (ICO) have separate roles and responsibilities. The Scottish Information Commissioner is responsible for the freedom of information compliance of all public authorities in Scotland, while the ICO is responsible for public authorities in England, Wales, and Northern Ireland, and for any agencies operating in both Scotland and another part of the UK. The ICO also covers Data Protection rights (personal information) for the whole of the UK, including Scotland.

The (UK) GDPR provides the following rights for individuals:

1. The right to be informed
2. The right to access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

5. General Guidelines

5.1. Example Step 1

5.2. **Perthshire Wellbeing Project** will, through appropriate management, strict applications of controls ensure:

- Confidential information is not shared informally
- Personal data is not disclosed to unauthorised people
- Collect and process appropriate information, only to the extent that is needed
- Employees keep all data secure and is only available to those who need it
- Strong passwords are used and regularly changed
- Appropriate security measures are in place to safeguard personal data
- Data is regularly reviewed, updated and archived in line with guidance and schedules
- When working with personal data, employees ensure screens of their computers are always locked when left unattended
- Hold good quality of information ensuring accuracy of data
- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data
- Training and assessment materials are kept on secure internal systems that are password protected. Printed assessment materials are locked in secure areas and only available to those intended
- Data is not transferred outside of the European area without suitable safeguards

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained
- Everyone managing and handling personal information is appropriately supervised
- Anybody wanting to make enquiries about personal information knows the process
- Enquiries are promptly and courteously dealt with
- Ensure that the rights of people about whom information is held can be fully exercised under the Act
- Methods of handling personal information are clearly described
- Methods of handling personal information are regularly reviewed, assessed and evaluated
- Data protection risks are monitored through Perthshire Wellbeing Project risk register
- Any breach of the rules and procedures identified in this policy is a potential breach of the Code of Conduct and may lead to disciplinary action.

6. Data Storage

6.1. Perthshire Wellbeing Project will ensure:

- Paper, CD, DVD files are kept in a locked drawer, when not required
- Printouts are not left where unauthorised people could see them
- Data printouts are shredded and disposed of securely when no longer required
- Electronic data is protected from unauthorised access and accidental deletion
- Passwords are changed regularly
- Data is backed up regularly
- Servers and computers are protected by approved security software
- Data is held in as few places as necessary
- Makes every effort to ensure that data held is accurate and kept up to date
- Regularly review data that is collected and cleansing of databases
- Regular archiving of data.

7. Data Sharing

All documents created by Perthshire Wellbeing Project are checked for accessibility and compatibility prior to public sharing; documents are also inspected for sensitive and personal data within:

- Comments, revisions, version, annotations
- Document properties and personal information
- Customised ML data
- Invisible content
- Hidden text.

8. Privacy Statement

Perthshire Wellbeing Project is committed to protecting the privacy and confidentiality of information provided by ‘users’ who access our website.

In order for ‘users’ to use some of our online services and to respond to enquiries we need to collect and process various personal data. Users may be asked to complete an online form(s) which request, name, address, e-mail and telephone number. The personal data we collect is used to process your request for our services.

By submitting personal information, individuals consent to Perthshire Wellbeing Project processing personal information in accordance with our data protection policy. All information provided will be treated as confidential and will only be used for the purpose intended. Anyone can contact Perthshire Wellbeing Project to correct or update personal information in our records.

We may use cookies on our website. Users may disable the use of cookies, but this may limit the function of the website. The site and our computer systems have security measures in place with the aim of protecting the loss, misuse or alteration of the information ‘users’ provide to us.

9. Process Steps

An individual is entitled to be given a description of the data being processed or held about them and to be provided with the information constituting personal data and the source.

9.1. Perthshire Wellbeing Project will supply information where:

- A request in writing has been made
- We are satisfied as to the identity of the applicant
- We are able to locate the requisite data.

Where these criteria have been met we will comply within **20 working days**. Where complying with the request would lead to disclosing data about another identifiable person we are not able to comply unless the other individual has consented or it is reasonable to comply without consent.

Where Perthshire Wellbeing Project has previously complied with a request, subsequent or similar requests for data will not be supplied unless a ‘reasonable interval’ has elapsed. As a non-public body, Perthshire Wellbeing Project is not covered by the Freedom of Information Act.

10. Archiving and Retention

Perthshire Wellbeing Project has an obligation, in line with the data protection policy, to implement and preserve good archiving procedures and processes. Archival records can be in any format; they can exist electronically or paper versions.

10.1. Files are summarised as:

- Operational files - that are in use daily
- Reference files - that are not in use daily, but are used for reference
- Inactive files - that are no longer active
- Remove files - that are removed after a period of inactiveness
- Preserved files – that are preserved permanently or for a specified length of time.

Perthshire Wellbeing Project aims to ensure:

- All records that are kept as archives will be included in a records retention log
- All records that are kept as archives will have a review date
- The length of their retention will be appropriate to the record – normally 3 years for training / assessment documents and normally 7 years for financial records
- Adhere as far as possible to BSI recommendations for the keeping of its archival records
- Individual staff members are responsible for the management of archival records in their areas of work.

10.2. Email Archive and Retention

- Messages will move to the online archive 18 months from the original send/receive date
- Messages will be deleted from the online archive 5 years from the original send/receive date
- Exceptions: Items in 'Deleted Items', 'RSS Feeds', and 'Sync Issues' folders will be deleted after 90 days.
- Electronic archive folders will be backed up regularly to ensure that they do not get lost.

11. Access to data

Perthshire Wellbeing Project will provide the Regulators, within a reasonable notice period (usually 7 days), access to premises, people and records as required, and fully cooperate with their monitoring activities, including those requested by Lantra.

12. Laptop/Home-working guidance/Personal Equipment

- Use the laptop as a dial-in facility where possible to minimise the information and work stored on the hard drive of the laptop
- Do not put personal data on a laptop
- Do not send reports or information to home computers via the internet unless you are using a secure connection
- Do not download reports or information onto removable storage devices to take work at home
- Do not take data relating to contacts out of the office. This includes internal and external contacts; hardcopy and softcopy files must not be kept at home. Information must not be kept on company mobile phones.
- If data relating to contacts is held/stored outside of the office environment then all personnel must take appropriate security measures to safeguard personal information.

If personal details relating to contacts is held/stored on equipment that does not belong to Perthshire Wellbeing Project (this includes information as basic as a name, phone number or address) it is up to the member of staff to ensure that nobody else has access to that

This policy is reviewed regularly and updated annually or as and when required.

Notes to understand and implement

(UK) GDPR and DPA applies to **'Data Controllers**' and '**Data Processors**' of an individual's personal data.
A **Data Controller** determines the purposes and means of processing personal data.
A **Data Processor** is responsible for processing personal data on behalf of a data controller.
If you are a **data processor**, the (UK) GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities.
You will have a legal liability if you are responsible for a breach.
However, if you are a **data controller,** you are not relieved of your obligations where a data processor is involved – the (UK) GDPR places further obligations on you to ensure your contracts with data processors comply with the (UK) GDPR.
The (UK) GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Personal Data
(UK) GDPR and DPA applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The (UK) GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
It is recommended you start by reviewing all the personal data you hold including the method of retaining the data either electronically or hardcopy.

- Consider why you hold the data and how long for.
- If you are holding personal data for any reason other than its original purpose, you may need the consent of the individual.
- If you are holding data for legitimate business interests ensure this has been explained to your data subjects (individuals). Advise them why you hold the data and for how long, how it will be disposed of and what their individual rights are.
- Review how secure your IT systems and hardcopy filing systems are – conduct a risk assessment and consider how you might mitigate a data breach.
- If you have a website, review your privacy policy to encompass (UK) GDPR

The ICO document **12 Steps to take now** is helpful in getting you started.
https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

The (UK) GDPR provides the following rights for individuals:

9. The right to be informed
10. The right to access
11. The right to rectification

12. The right to erase
13. The right to restrict processing
14. The right to data portability
15. The right to object
16. Rights in relation to automated decision making and profiling.

The information you must supply

The information you must supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible.
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

When obtaining data directly from individuals you must supply the following information:

- Identity and contact details of the data processor
- Purpose of the processing and the lawful basis for processing
- The legitimate business interest of the data controller or third party – where applicable
- Any recipients of the personal data
- Details of any transfers to a third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of individuals rights
- The right to withdraw consent at any time
- The right to lodge a complaint with the supervisory authority – in the UK this is the Information Commissioner's Office (ICO).
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide personal data.
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
https://www.oireachtas.ie/en/bills/bill/2018/10/

This policy is reviewed regularly and updated annually or as and when required.
