Planning Aid **Wales**
Cymorth Cynllunio **Cymru**

Data Protection Policy and Procedure (compliant with the GDPR)

Policy Status:	Published v3
Approved by:	PAW Management Board
Date:	17th September 2018

Table of Contents

1. Purpose

1.1 Planning Aid Wales (PAW) is committed to being transparent about how it collects and uses personal data and sensitive personal data relating to job applicants, employees, former employees, donors, trustees and volunteers, and to meeting its data protection obligations. This policy sets out PAWs' commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 This policy applies to the personal data of job applicants, employees, former employees, donors, trustees and volunteers. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

1.3 PAW has appointed the Chief Executive as its data protection officer. His role is to inform and advise PAW on its data protection obligations. He can be contacted at james@planningaidwales.org.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

2. Definitions

2.1 **"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2.2 **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

2.3 **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data Protection Principles

3.1 PAW processes HR-related personal data in accordance with the following data protection principles:

3.1.1 PAW processes personal data lawfully, fairly and in a transparent manner;
3.1.2 PAW collects personal data only for specified, explicit and legitimate purposes;
3.1.3 PAW processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;

3.1.4 PAW keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
3.1.5 PAW keeps personal data only for the period necessary for processing;
3.1.6 PAW adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

3.2 PAW tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

3.3 PAW will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.4 Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on PAW's HR system. The periods for which PAW holds HR-related personal data are contained in its privacy notices to individuals.

3.5 PAW keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Individual Rights

Subject Access Requests

4.1 Individuals have the right to make a subject access request. If an individual makes a subject access request, PAW will tell him/her:

4.1.1 whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
4.1.2 to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
4.1.3 for how long his/her personal data is stored (or how that period is decided);his/her rights to rectification or erasure of data, or to restrict or object to processing;
4.1.4 his/her right to complain to the Information Commissioner if he/she thinks PAW has failed to comply with his/her data protection rights; and
4.1.5 whether or not PAW carries out automated decision-making and the logic involved in any such decision-making.

4.2 PAW will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise. If the individual wants additional copies, PAW may charge a fee, which will be based on the administrative cost to PAW of providing the additional copies.

4.3 To make a subject access request, the individual should send the request to james@planningaidwales.org.uk. In some cases, PAW may need to ask for proof of identification before the request can be processed. PAW will inform the individual if it needs to verify his/her identity and the documents it requires.

4.4 PAW will normally respond to a request within a period of one month from the date it is received. In some cases, such as where PAW processes large amounts of the individual's data, it may respond within three months of the date the request is received. PAW will write to the individual within one month of receiving the original request to tell him/her if this is the case.

4.5 If a subject access request is manifestly unfounded or excessive, PAW is not obliged to comply with it. Alternatively, PAW can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely found to be manifestly unfounded or excessive where it repeats a request to which PAW has already responded. If an individual submits a request that is unfounded or excessive, PAW will notify him/her that this is the case and whether or not it will respond to it.

5. Other Rights

5.1 Individuals have a number of other rights in relation to their personal data. They can require PAW to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where PAW relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask PAW to take any of these steps, the individual should send the request to james@planningaidwales.org.uk.

6. Data Security

6.1 PAW takes the security of individual personal data seriously. PAW has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. All breaches of security will be investigated should they occur.

6.2 Personal or sensitive personal data can only be disclosed to authorised persons on a need to know basis and with the consent of the individuals concerned. No personal or sensitive personal data can be disclosed without authorisation from the Data Protection Officer.

6.3 All information kept on authorised computers will be password-protected. Backup copies of information stored on computers will be made regularly and will be kept off-site in a secure place.

6.4 Papers sent to interviewers must be kept in a secure place and only accessible to authorised personnel. All such papers will be collected after the interviews and shredded.

6.5 Information provided to PAW will be destroyed as soon as it is no longer needed. Personal and sensitive personal data will only be kept as long as is necessary. All personnel involved in any way with the handling of personal and sensitive personal data will be trained on PAW's data protection policies, security systems and procedures.

6.6 Where PAW engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7. Impact Assessments

7.1 Some of the processing that PAW carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, PAW will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8. Data Breaches

8.1 If PAW discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. PAW will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

9. International Data Transfers

9.1 PAW will not transfer HR-related personal data to countries outside the EEA.

10. Individual Responsibilities

10.1 Individuals are responsible for helping PAW keep their personal data up to date. Individuals should let the organisation know if data provided to PAW changes, for example if an individual moves house or changes his/her bank details.

10.2 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, PAW relies on individuals to help meet its data protection obligations to staff and to customers and clients.

10.3 Individuals who have access to personal data are required:

10.3.1 to access only data that they have authority to access and only for authorised purposes;

10.3.2 not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;

10.3.3 to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

10.3.4 not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

10.3.5 not to store personal data on local drives or on personal devices that are used for work purposes.

10.4 Further details about the organisation's security procedures can be found in its **Data Security Policy**.

10.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's **Disciplinary Policy and Procedure**. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11. Training

11.1 PAW will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

11.2 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

12. Handling Special Category or Criminal Records Data

12.1 In the case of volunteers, the organisation will collect special category data with consent from the individual and this data will be collected and stored anonymously or using pseudonyms.

12.2 Any special category data held on service users that are linked to files will be securely held in the client management database.

12.3 Employee special category data is collected and processed for the following reasons:

- the purposes of performing or exercising obligations or rights of the employer or employee under employment law, such as not to discriminate against an employee or dismiss them unfairly;
- establishing, exercising or defending legal claims; or
- the assessment of an employee's working capacity, subject to confidentiality safeguards.

12.4 Completion of a health surveillance form at the beginning of employment will be discretionary and will only be completed by the employee with explicit consent.

12.5 Any special category data held on employees will be securely held on the employee database and management drive of the shared server.

12.6 In order to protect the clients that the organisation supports, it is a requirement of employees, trustees and volunteers to have a Disclosure and Barring Service (DBS) check.

12.7 The required information from identity documents and the DBS check will be entered into the HR system and the original documents destroyed.

13. Document Details

13.1 **Document History**

Version Number	Published v3.0
Date approved	
Approved by	
Next review due	
Who this policy applies to	Job applicants, employees, former employees, clients, donors, trustees and volunteers.
Who is responsible for the policy	The Chief Executive
Links with legislation	• General Data Protection Regulation (2016/679 EU) • Data Protection Act 1998 • Data Protection Bill
Links with other policies	• Policy on Data Subject Rights • Policy on the Secure Storage, Handling, Use, Retention and Disposal of Disclosure and Barring Service (DBS) Certificates and Certificate Information • Disciplinary Policy and Procedure

13.2 All enquiries with regard to this document should be addressed to the Chief Executive. Expired issues of this document will be retained by the Chief Executive and Heard HR Solutions Ltd.

13.3 This policy and procedure will be reviewed every three years, unless:

- There are significant changes to legislation or regulation
- There are found to be deficiencies or failures in this policy and procedure which result in complaints from managers or staff members
- The policy and procedure is deemed to be no longer effective or in line with business requirements

At which point, the Chief Executive will initiate an immediate review.

13.4 Revision History

Version 1.0	Oct 2012	PAW	Approved version
Draft 2.0	Mar 2018	Heard HR Solutions Ltd	Draft Amendments
Draft 2.1	May 2018	Heard HR Solutions Ltd	Draft Amendments Adopted by SAC 25th May 2018
Draft 2.2	September 2018	Chief Executive	Final amendments
Published 3.0	September 2018	PAW Management Board	Adopted full Policy