1.0 Scope

Haulfryn needs to gather and use certain information about individuals.

These can include service users, next of kin, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Company's data protection standards and to comply with the law 'UK Data Protection Act 2018'.

Haulfryn is registered with the Info Commissioner's Office Registration Number ZA087561.

Why this Policy Exists

The data protection policy ensures Haulfryn:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of data breach

UK Data Protection Law

The UK Data Protection Act 2018 and The General Data Protection Regulations (GDPR) describes how organisations – including Haulfryn, must collect, handle and store personal information.

Personal data is defined as any information relating to an identified or identifiable person.

These rules apply regardless of whether data is stored electronically, on paper or other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The UK Data Protection Act is underpinned by six important principles. These are:

- Lawfulness Fairness and Transparency – Information must be processed lawfully, fairly and in a transparent manner.
- Purpose Limitation – Data must be collected for specified, explicit and legitimate purposes.
- Data Minimisation – Data must be adequate, relevant and limited to what is necessary.
- Accuracy – Data must be accurate and, where necessary, kept up to date.
- Storage Limitation – Data must be retained only for as long as necessary.
- Integrity and Confidentiality – Data must be processed in an appropriate manner to maintain security.

Roles and Responsibilities

- Controller – Haulfryn determines the purposes and means of the processing of personal data.
- Data Protection Officer – The Manager, Clare Roberts, is the individual who informs and advises staff members about their obligations to comply with the GDPR, monitor compliance with the GDPR, train staff and conduct internal audits.
- Data Subject – all individuals whose data is stored, i.e. the service user, next of kin, business contacts.

Special Categories of Data

Under GDPR, special categories of personal data are more sensitive and require a greater degree of protection. Examples of special categories of personal data include information about an individual's:

- Race
- Ethnic origin
- Political beliefs
- Religion
- Genetics
- Health
- Sex life
- Sexual orientation
- Criminal record

Policy Scope

This policy applies to:

- All staff and volunteers of Haulfryn
- All contractors, suppliers and other people working on behalf of Haulfryn

It applies to all data that Haulfryn holds relating to identifiable individuals, even if that information technically falls outside of The UK Data Protection Act 2018. This can include:

- Names of individuals
- Postal address
- Email address
- Telephone numbers
- Plus any other information relating to individuals

Data Protection Risks

This policy helps to protect Haulfryn from some very real data security risks, including;

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Haulfryn has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key area of responsibility:

The Directors are ultimately responsible for ensuring that Haulfryn meets its legal obligations.

Clare Roberts Manager is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Renewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Haulfryn holds about them (also called 'Data Subject Access Request').
- Checking and approving any contracts or agreement with third parties that may handle the Company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meets acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third party services the Company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Personal data **should not be disclosed** to unauthorised people.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer

required, it should be deleted and disposed of within the set guidelines from CIW.

Data Storage

These rules described how and where data should be safely stored. Questions about storing data safely can be directed to Clare Roberts, manager or Peter Regan, Responsible Individual.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required, the papers or files should be **kept in a locked drawer or filling cabinet**.
- Employees should make sure papers and printouts **are not left where unauthorised people could see them,** for example in a communal area.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives, and servers** and should only be updated to an **approved cloud computing services.**
- Data should be backed up frequently. Those backups should be tested regularly in line with Company's standard back up procedures.
- All servers and computers containing data should be protected **by approved security software and firewall.**

Data Use

Personal data is of no value to Haulfryn unless the business can make use of it, however it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally, in particular it should never be sent by email as this form of communication is not secure, unless an email address has been confirmed.

Data Accuracy

The law requires Haulfryn to take reasonable steps to ensure data is kept accurate and up to date.

It is important to ensure that the personal data we store is accurate.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary
- Staff take every opportunity to ensure data is updated
- Data should be updated as inaccuracies are discovered. For instance, if a next of kin should be removed from the support plan

Data Subject Access Requests

All individuals who are the subject of personal data held by Haulfryn are entitled to:

- Ask **what information** the Company holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Be informed how the Company is **meeting its data protection obligations**

If an individual contacts the Company requesting this information, this is called a Data Subject Access Request.

Data Subject Access Requests from individuals should be made by email, addressed to the data controller at info@haulfryn-care.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per Data Subject Access Request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a Data Subject Access Request before handling over any information.

Disclosing Data for Other Reasons

In certain circumstances the UK Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Haulfryn will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from legal advisers where necessary.