



Privacy Notice

County Durham Floating Support

This privacy notice is for County Durham Floating Support which is a service Waythrough provide in Durham. We are funded by Durham County Council to provide this service.

Waythrough adheres to the Data Protection Act 2018 in relation to how we collect and process information that identifies you as an individual. This type of information is called personal data.

Managing Your Information

Waythrough is the Data Controller for County Durham Floating Support which means that we decide how data is processed and the purpose for the processing. We are accountable for ensuring that your rights are respected and that the data is processed lawfully. Should a breach occur, it is our responsibility to report it to the Information Commissioner's Office (ICO) if there is a high risk to your rights or freedoms as per the UK General Data Protection Regulation (UK GDPR).

What We Use and Why

We use personal data like your name, address and contact details so that we can provide you with a service.

We also use more sensitive data about your health; and demographic data such as your gender, sexual health (specifically relationships), sexual orientation, race and ethnicity and religious beliefs]. This is called **Special Category Data** which requires extra protection.

If you are subject to the criminal justice system, we may process some criminal offence data about you so that we can provide you with our service and so that we can manage risks to you, to our team and to the public.



How We Collect Your Data

We receive your data from you and sometimes from other people like your local authority, Children and Adult social care services, the police and probation services].

We may receive your data by telephone, email, electronic web form or by post.

Lawful Reasons for Processing.

The lawful reasons (known as lawful bases) for processing are set out in the UK General Data Protection Regulation (UK GDPR). At least one of these must apply whenever we process personal data.

We use the lawful basis of **Legitimate Interests** to process your data, to provide you with the service.

Where we deliver community orders (such as ATR, DRR, CBO or civil injunctions) we may also process your data upon a **Public Task**.

We process your health data using the **Health or Social care condition of the UK GDPR**. We only process what is necessary for the purpose; and processing is overseen by a health professional bound by the common law duty of confidentiality.

In addition to health data, we process a minimal amount of other special category data such as data about your racial or ethnic origin, religious or philosophical beliefs, sex life, sexual orientation/relationships and we use this data for demographic purposes and statistical analysis and to meet individual health and social care needs

Where we are processing criminal offence data, we rely on special conditions under the Data Protection Act 2018 relating to health and social care, preventing or detecting unlawful acts and safeguarding.

Sharing Your Information with Others (also known as 'Third Parties')

There are times when we may share data in the public interests relying on the basis of **Public Task** or because it is our **Legal Obligation** to share your information with third parties (usually authorities) and we do not require your consent to be allowed to do this. Sometimes we do not need to make you aware that we are sharing. We will only share the information that is needed; and we only share the minimum information for the purpose.



Examples of this are:

- to report a crime to the police (this includes driving under the influence)
- to report abuse or neglect to social services
- to let mental health crisis services know if you are at serious risk
- to share information in multiagency settings should you be subject to Multi Agency Risk Assessment Conferences (MARAC: to prevent domestic abuse) and/or Multi Agency Tasking and Coordination Meetings (MATAC: to prevent domestic abuse), or Multi Agency Public Protection Arrangements (MAPPA: to prevent reoffending).
- we must share data with the Care Quality Commission (CQC) who are a regulatory body. Wherever possible we anonymise data, but sometimes we are required to share personal data when a serious incident has occurred.
- any other request where we are obliged to share data as per a legal obligation which is laid down in UK law.

Where we deliver community orders (such as ATR, DRR, CBO or civil injunctions) we may also process your data upon a **Public Task** and **Legitimate Interests** when we share with the authorities. In all cases there is a legal requirement for us to use and share your data.

We rely on the lawful basis **Legitimate Interests** to share your personal data with:

- the local authority social care team to provide you with support through partnership working, where risks and vulnerabilities require us to do so in your best interests or in the best interests of others (particularly children, families and adults at risk).
- we may share information to your GP where we make the decision that your life or someone else's is at risk, and we believe strongly that the GP is in a key position to help you/others. If we make this decision, we will make all reasonable attempts to inform you.
- the prison, probation services, courts and police to share prescribing information and/or arrange ongoing support, if you have recently been released or are going into custody.

If our project is decommissioned, we will transfer all your data to the new provider and notify you by letter. We transfer your data on the lawful basis of legitimate interests so that you continue to receive the service you are using. Although we transfer your data, we also keep a copy of your data in line with our retention period (see below "Keeping Your Information").



All other third-party personal data sharing is decided by you with your explicit consent. You provide us with this information on the **Sharing Consent Process**. You should update us at any point if you wish us to change these consents.

Confidentiality

Information about you may be shared between team members; and recorded on your file and in other records to enable us to give you the best service that we can and get the best possible support for you.

Only what is necessary and proportionate is shared and we are bound by the common law duty of confidentiality. In some circumstances we may share your data in order to keep you or other people safe which is a legal obligation this is explained in the section above titled **Sharing Your Information with Third Parties**.

Transferring Your Data Outside of the UK

As part of our day-to-day operations, we do not transfer your data outside of the UK unless with your explicit consent to do so (right to portability).

When a service closes and we archive data in line with our data retention period, we use a third-party Processor called Iron Mountain. Iron Mountain may in some instances, use sub-processors who are based in other countries. Iron Mountain ensures that where required, Standard Contractual Clauses are in place to protect data where it is transferred to another country as per the EU's adequacy decisions.

Keeping Your Information Safe

Your data is held securely on a third-party management system and only those who need access, have access to it. This includes staff that support you and staff who maintain the system. We have policies in place which our staff follow to ensure your data is only accessed appropriately and when necessary.

We store some of your personal data on our secure network drives which is restricted to our service team and may be accessed under policy by our IT Team should there be a technical issue. All Waythrough workforce abide by data management policies, processes and training.



We cannot offer you a service without storing your details on these systems.

We have a number of people who oversee that data is used safely (see 'Relevant Contacts').

Should an incident occur where we breach your data, causing a high risk to your rights or freedoms, we will inform you of this without delay and using the primary contact details you have provided. We will also report this to the Information Commissioner's Office (ICO), who supervise organisations that handle data.

Retaining Your Information

We keep your personal data for the period stated in our records retention and destruction policy. The policy currently states that we will keep your information for 10 years from the date that the service contract ends which for this service is currently 31/03/2024.

Your data will be securely destroyed at the end of our retention period.

In the event that we change the retention period in our policy, we will update our privacy notice and notify you of this change.

Keeping in Touch with You

As part of your support, we will contact you at various stages to discuss your progress, deliver interventions and provide reminders around upcoming appointments.

This is usually via the following methods; however, this is not an exhaustive list:

- letters
- online platforms such as Zoom or WhatsApp
- phones calls
- home visits (when applicable)
- e-mails*
- text messages*

If you do not wish to be contacted via one or all of these methods or have specific communication needs, then please tell us using the **Contact Preferences** form. You can request this from your Waythrough worker.



*e-mail & text Messages should be used for non-urgent contact only. Recovery Coordinators have e-mail accounts and mobile phones but will not routinely access them throughout the day. We always recommend phoning the service if you require assistance urgently (for example cancelling / rearranging upcoming appointments).

Your Data Rights

Under the Data Protection Act 2018 and UK GDPR, you have the following rights:

- to be informed about the collection and use of your personal data.
- to access your personal data (known as Subject Access Request).
- to have inaccurate personal data rectified; or completed if it is incomplete.
- to have personal data erased (known as the right to be forgotten).
- to request the restriction or suppression of your personal data.
- to data portability, which allows individuals to obtain and reuse their personal data for their own purposes across different services.
- to object to the processing of your personal data in certain circumstances.

We do not use any automated decision making (decisions made by a computer) or profiling (when an automated system is used to assess certain things about you) when we use your data.

Please note that some of these rights only apply in certain situations and we may not be able to fulfil every request. Where we say no to a request, we will always explain our decision in full, within the timeframe that the law says. Should you request that your data is erased please be aware that we will be unable to continue offering you a service as we require your personal data to do this effectively and safely.

To request access to your data or to contact us about any of the rights we have listed, you can request this through the service or contact our Caldicott Guardian (see below; Relevant Contacts).



How To Complain

If you are unhappy about an issue relating to your data you can complain to us through the service you attend; or if you would feel more comfortable, you can contact the Waythrough Caldicott Guardian (see below; Relevant Contacts).

To make a formal complaint to the independent regulator for personal data in the UK about the way we have used your data, contact the Information Commissioner's Office (ICO):

- <https://ico.org.uk/make-a-complaint/> or call ICO on 0303 123 1113

Relevant Contacts

You can write to us at Waythrough, Inspiration House, Unit 22 Bowburn North Industrial Estate DH6 5PF.

Our Data Protection Officer (DPO) is Mark Burnett. You can contact our DPO by email dpo@waythrough.org.uk or by phone 01325 731 160.

Our Caldicott Guardian is Leesa Howes. You can contact our Caldicott Guardian by email caldicott.guardian@waythrough.org.uk or by phone 01325 731 160.