Community Diversion Service Privacy Notice

This privacy notice is for Community Diversion service users. Community Diversion is a service Humankind provide in Newcastle, Gateshead, North Tyneside, South Tyneside, Northumberland and Sunderland. We are funded by Northumbria's Violence Reduction unit to provide this service.

Humankind 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.

Please note: If you started using our services prior to 1st October 2022, this privacy notice does not apply and you should request a copy of the information you received at the time from the service. You can also contact Caldicott.guardian@humankindcharity.org.uk

Managing Your Information

Humankind is the **Data Controller** for Community Diversion Service 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 **Article 9 condition (h) Health or Social care**. 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. This is further supported by **Schedule 1 Condition 2; Health and Social Care Purposes.**

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 two clear purposes. We have outlined these below and their relevant Article 9 conditions:

- For demographic purposes and statistical analysis. Upon condition ((j) Archiving, research and statistics (with a basis in law). This is further supported by Schedule 1 Condition 4; Research.
- To meet individual health and social care needs Article 9 condition (h) Health or Social care. This is further supported by Schedule 1 Condition 2; Health and Social Care Purposes.

Where we are processing criminal offence data, we rely on:

- the Schedule 1, Condition 2; **Health and Social Care Purposes** to work with the prison and probation to provide you with healthcare.
- the Schedule 1, Condition 10; **Preventing or Detecting Unlawful Acts**, if there is a high risk of reoffending and we need to manage risks in relation to the public.
- the Schedule 1, Condition 18; **Safeguarding Children and Individuals of Risk**, to manage risks where you may present a risk to the public and service users we work with.

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
- if you are on a criminal justice order we will inform your Offender Manager or Probation Officer of your engagement.

- 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).
- to share information (if requested to by law) with the court of law.
- 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.

If you were in a life-or-death situation, we use the lawful basis **Vital Interests** to provide your personal data to the emergency services so that they may save your life.

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 Form**. You should update us at any point if you wish us to change these consents.

Management Information Systems (MIS)

The service uses a third-party MIS called, Charity Log. Your data is held securely and only those who need access, have access to it. This includes staff that support you and also 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 also have an incident reporting system called the Hub. This is where we record incidents such as safeguarding, death in service, health and safety and information governance incidents. We would only add your personal data to this system if you were involved in an incident. Each incident has access restrictions. Only those who are interested parties can see it and some staff who maintain the system.

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

We also use paper records and we store these in a secure manner with access limited only to those who need it.

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

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

We keep your information safe by using secure ways to store it. We only keep what we need and no more than that. Everyone who handles data is trained on how to use it safely and only people who need to use it are able to.

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.

Keeping 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 01/03/2026.

Our service is commissioned for the time period stated above. If we are recommissioned, our contract will be extended. If you stop using our service before we are recommissioned, we will retain your data for the time stated above. If we are recommissioned and you continue to use our service, we will extend the retention date to be 10 years after the end date of the recommissioned service. We will write to inform you of any changes to our retention period. If you do not have a postal address, we will attempt to inform you by other contact methods.

If we are decommissioned we will share your data as a legitimate interest to the new provider and we will delete your information 10 years from the contract end date.

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

Destroying Your Information

Your data will be securely destroyed at the end of our retention period. It will be destroyed by us if it is electronic. Where we hold paper records, we will use a contractor who will destroy this data on our premises. If destruction is required after data has been archived with a third-party information management provider called Iron Mountain. Iron Mountain act as a Data Processor for Humankind under contract.

Keeping in Touch With You

As part of your treatment 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 Process**. You can request this from your Humankind 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 Humankind 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 Humankind, Inspiration House, Unit 22 Bowburn North Industrial Estate DH6 5PF.

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

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