Insight Royal Borough Kensington and Chelsea & Westminster

Privacy Notice

This privacy notice is for people who use **Insight Royal Borough Kensington and Chelsea & Westminster (Insight RBKCW)**. **Insight RBKCW** is a service Humankind provide in the London Boroughs Kensington and Chelsea & Westminster. We are funded by RBKCW local authorities 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.

Managing Your Information

Humankind is the **Data Controller** for **Insight RBKCW** 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 personal data called **Special Category Data** which requires extra protection. The special categories we process about you include:

- Health: to provide you support, advice and access to treatment.
- Racial or ethnic origin: for demographic purposes and statistical analysis.
- Religious or philosophical beliefs: to meet your individual needs, for demographic purposes, statistical analysis and some legal obligations.
- Sex life: to provide you with support, advice, access to health interventions and to comply with safeguarding law.
- Sexual orientation: to meet your individual needs, for demographic purposes and statistical analysis.

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 school, Youth Offending Service, National Probation Service, GP, local authority, Primary Care Service and other Services. Anyone can refer you into our service.

We may receive your data by telephone, email 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 and for our retention purposes.

We process the special category data listed above 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.**

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.
- any other request where we are obliged to share data as per a legal obligation which is laid down in UK law.

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:

- Sexual health services in order to improve your health and to reduce risks to you
- 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).
- your GP, in order to ensure safe prescribing.
- pharmacies, in order to support safe prescribing.
- 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 arrange ongoing support, if you have recently been released or are going into custody.
- research organisations and funders who carry out evaluation and statistical work. Your data is only shared for research and planning purposes with Caldicott Guardian Approval following our National Data Opt Out Policy. Please see the section below 'You Can Opt Out of Your Personal Data Being Used For Research and Planning' which explains this in more detail.
- adult community drug and alcohol services, to access and ensure safe prescribing up to the age of 25 and to enable transition to such services should you reach the upper age limit of the service and require ongoing support.

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").

We do not need your consent to use or share your data when we rely on legitimate interests, but we do need to make sure processing is secure, ethical, necessary and proportionate. Please note that you have the right to object to any processing which is carried out on legitimate interests (see Your Data Rights section below) but we can refuse to agree to your objection.

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.

The **Sharing Consent Form** will ask you if you wish us to share your data with NDTMS. NDTMS is the National Drug Treatment Monitoring System (NDTMS). It is used by the Office for Health Improvement and Disparities (OHID) to collect information about drug and alcohol treatment in

England. If you consent, your treatment service will share some of your treatment information with NDTMS.

You Can Opt Out of Your Personal Data Being Used For Research and Planning

National Data Opt Out is a government policy overseen by the NHS. Humankind Charity is one of many organisations working in the health and care system to improve care for patients and the public. Whenever you use a health or care service, such as a Humankind health or social care service, attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this where allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified, in which case your confidential patient information isn't needed.

Where your data cannot be anonymised and Humankind Charity is not confident that you are aware that your personal data may be used for research or planning, Humankind will generally seek to obtain your explicit consent. However, by providing you with this privacy notice and making you aware of National Data Opt Out, Humankind is letting you know that we may on occasions use or share your data for research of planning purposes without your consent, based upon a legitimate interest.

Where Humankind has your NHS number, we can check to see if you have applied an **NHS Opt Out** to your data being used for this purpose. Patients apply their Opt Out via the NHS National Data Opt Out process. If you have Opted Out, Humankind Charity will not use or share your data for purposes other than your treatment and care (i.e. Humankind Charity will not use or share your data for research or planning).

You have a choice about whether you want your confidential patient information to be used for research and planning. If you are happy with this use of information you do not need to do anything. **If you do choose to Opt Out of your data being used for research or planning, your confidential patient information will still be used to support your individual care.**

To find out more or to register your choice to Opt Out, please visit the NHS website www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

https://www.hra.nhs.uk/information-about-patients/ (which covers health and care research); and https://understandingpatientdata.org.uk/what-you-need-know (which covers how and why patient information is used, the safeguards and how decisions are made)
You can change your mind about your choice at any time.

Please Note: Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement. There are also other exemptions when Humankind does not need apply Opt Out and these can be reviewed here

Management Information Systems (MIS)

The service uses a third-party MIS called, SystmOne. 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 cannot offer you a service without storing your details on 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 securely 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.

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 30th June 2023.

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 or by a Data Processor whom we will contract in line with Article 28 of the UK GDPR.

If destruction is required after data has been archived, Iron Mountain provide this service 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 attend an appointment we may post a letter to your home address to notify you.

If you do not wish to be contacted via one or all of these methods or have specific communication needs then please tell us. You can request this from your Humankind worker.

When contacting us 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. This right does not apply to processing done on legitimate interests.
- to object to the processing of your personal data in certain circumstances.
- to withdraw consent where your consent is the lawful basis of processing.

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 contact us at insight@humankindcharity.org.uk or call us at 0208 960 5510

Alternatively 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.