Recruitment Privacy Notice

1 Overview

1.1 Cumbria Health whose registered office is 4 Wavell Drive, Rosehill Industrial Estate, Carlisle, CA1 2SE is a **Data Controller**. This means that we determine the purpose and means of the processing of your Personal Data.

1.2 Cumbria Health is required to appoint a Data Protection Officer (DPO) in respect of our processing activities. Cumbria Health uses an external DPO whose details are set out below:

Yvonne Salkeld
Head of Information Governance
North Cumbria Integrated Care
Maglona House, Unit 68, Kingstown Broadway, Carlisle, CA3 0HA
Tel: 01228 603927

You should contact the DPO if you have any concerns about the information contained in this privacy notice or data protection within Cumbria Health generally.

1.3 Cumbria Health takes the security and privacy of your data seriously. We need to gather and use information about you as part of our business. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the Data Protection Act 2018 and the **EU General Data Protection Regulation** ("GDPR"). We have a legal obligation to provide the information contained in this notice.

1.4 Cumbria Health has measures in place to protect the security of your data in accordance with our Data Protection, Information Governance, Records Management, Information Security, and Email and Internet Use policies.

1.5 Cumbria Health will hold data in accordance with our Records Management Policy. We will only hold data for as long as necessary for the purposes for which we collected it.

1.6 This notice explains how Cumbria Health will hold and process your information.

1.7 It is intended that this privacy notice is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this notice, Cumbria Health intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This notice applies to all personal data relating to data subjects whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, someone else (such as your current employer, a former employer a background check provider (including the Disclosure and Barring Service) or a recruitment agent), a practice owned and/or operated by us or it could be created by us.

3.4 We will collect and use the following types of personal data about you:

- Name and address and contact telephone number;
- The information you have provided to us in your curriculum vitae and covering letter;
- Any information you provide to us during an interview (including test results and any documents we ask you to produce);
- Details of your referees and any references provided;
- Evidence of your right to work in the UK;
- Evidence of your qualifications.

4 How we define special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your religious or philosophical beliefs;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and

- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

We will use your special category data in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

- We will use the information you provide us with in relation to any criminal charges or convictions to determine your suitability for the role.

5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;

- adaption or alteration;

- retrieval, consultation or use;

- disclosure by transmission, dissemination or otherwise making available;

- alignment or combination; and

- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 Cumbria Health will process your personal data (including special categories of personal data) in accordance with our obligations under GDPR and the 2018 Act.

6.2 We will use your personal data to:

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.
- Comply with our obligations to make reasonable adjustments, if necessary.

6.3 It is in our legitimate interests to decide whether to appoint you to work for us since it is beneficial to our business to appoint appropriately qualified employees.

6.4 We also need to process your personal information to decide whether to enter into a contract of employment with you and to comply with our legal obligations.

6.5 Having received your CV and covering letter, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you a job. If we decide to offer you a job, we will then take up references and check you have the right to work in the UK. We will also carry out a DBS check.

6.6 We can process your personal data for these purposes without your consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

6.7 If you choose not to provide us with certain personal data you should be aware that we may not be able to offer you employment or progress your application.

6.8 We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing data.in relation to any criminal convictions you may have.

6.9 If we require your explicit consent for processing (which will be rare) then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting our DPO or informing the HR Manager.

6.10 We do not make automated decisions about you using your personal data or use profiling in relation to you.

7 Sharing your personal data

7.1 We will only share your personal information with any recruitment agents for the purposes of processing your application. All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

7.2 We do not typically transfer personal data outside the UK. We will only transfer your personal data out of the UK in the following circumstances:

- It is to countries that have been deemed to provide an adequate level of protection for personal data by the Secretary of State;
- Where we can ensure that appropriate safeguards are in place with the recipient in accordance with the Data Protection Act 2018; or

- The transfer is otherwise permitted pursuant to the Data Protection Act 2018

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

8 Subject access requests

8.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them.

8.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Cumbria Health. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

8.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

9 Your data subject rights

9.1 You have the right to information about what personal data we process, how and on what basis as set out in this notice.

9.2 You have the right to access your own personal data by way of a subject access request (see above).

9.3 You can correct any inaccuracies in your personal data. To do so you should contact our DPO.

9.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact our DPO.

9.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact our DPO.

9.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

9.7 You have the right to object if we process your personal data for the purposes of direct marketing.

9.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller in limited circumstances. We will not charge for this and will in most cases aim to do this within one month.

9.9 With some exceptions, you have the right not to be subjected to automated decision-making.

9.10 You have the right to be notified of a data security breach concerning your personal data.

9.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact our DPO.

9.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

10 Data Security

10.1 We have put in place measures to protect the security of your data. We will keep our working practices under review and update them as necessary to protect personal data.

10.2 Third parties will only process your data on our instructions and where they have agreed to treat the data confidentially and to keep it secure.

10.3 We have put in place appropriate security measures to prevent your data from being accidentally lost, used or accessed in an unauthorised way, altered or

disclosed. In addition, we limit access to your data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your data on our instructions and they are subject to a duty of confidentiality.

10.4 We have procedures in place to deal with any suspected data security breach and will notify you and the Information Commissioner's Office of a suspected breach where we are legally required to do so.

11 Data retention

11.1 We will only retain your data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are available in our Records Management Policy. Please contact our DPO if you would like to see a copy of our Records Management Policy. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Most personal data for unsuccessful job applicants will be destroyed after 6 months.

11.2 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.