

## **PRIVACY NOTICE – EMPLOYEES AND CANDIDATES**

### **1. POLICY STATEMENT**

- 1.1 Hailsham House is committed to protecting the privacy and security of your Personal Data. This policy describes how we collect and use Personal Data about you when you apply to work for us, as well as during and after your working relationship with us, in accordance with requirements under the General Data Protection Regulation (GDPR). It applies to all candidates, employees, workers, contractors, consultants, agency workers and volunteers.
- 1.2 Please notify us of any changes to your Personal Data so that we can keep it up to date.
- 1.3 We are a "data controller". This means that we are responsible for deciding how we hold and use Personal Data about you.
- 1.4 Hailsham House has appointed a data protection officer ("DPO") who is responsible for compliance with data protection legislation. The DPO is Will Graham.

### **2. DEFINITIONS**

"Personal Data" means any information about an individual from which that person can be identified.

"Processing" or "to Process" means any activity which involves the use of Personal Data, including recording, storing, sharing and deleting it. There must always be a legal basis for any Processing.

### **3. THE KIND OF INFORMATION WE HOLD ABOUT YOU**

- 3.1 We will collect, store and use the following categories of Personal Data about you:
  - 3.1.1 Personal contact details such as name, title, addresses, telephone numbers and personal email addresses.
  - 3.1.2 Date of birth.
  - 3.1.3 Gender.
  - 3.1.4 Marital status and dependants.
  - 3.1.5 Next of kin and emergency contact information.
  - 3.1.6 National Insurance number.
  - 3.1.7 Bank account details, payroll records and tax status information.
  - 3.1.8 Salary, annual leave, pension and benefits information.
  - 3.1.9 Start date.

- 3.1.10 Location of employment or workplace.
  - 3.1.11 Copy of driving licence.
  - 3.1.12 Recruitment information (including copies of right to work documentation, references, cognitive behaviour tests and other information included in a CV or cover letter or as part of the application process).
  - 3.1.13 Any information you provide to us during an interview.
  - 3.1.14 Employment records (including job titles, work history, working hours, training records, qualifications, registration numbers and professional memberships).
  - 3.1.15 Compensation history.
  - 3.1.16 Performance information.
  - 3.1.17 Disciplinary and grievance information.
  - 3.1.18 CCTV footage and other information obtained through electronic means.
  - 3.1.19 Information about your use of our information and communications systems.
  - 3.1.20 Photographs.
- 3.2 We may also collect, store and use the following "special categories" of more sensitive Personal Data:
- 3.2.1 Information about your race or ethnicity, religious beliefs and sexual orientation.
  - 3.2.2 Information about your health, including any medical condition, health and sickness records.
  - 3.2.3 Information about criminal convictions and offences.

#### **4. HOW IS YOUR PERSONAL DATA COLLECTED?**

We collect Personal Data about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. We will collect additional Personal Data in the course of job-related activities throughout the period of you working for us.

#### **5. THE LEGAL BASIS FOR OUR USE OF YOUR PERSONAL DATA**

- 5.1 By way of example, we will use your Personal Data for the purposes set out below, some of which will overlap.

**5.2 Processing for the purpose of deciding whether to enter into a contract with you (or an agency acting on your behalf)**

5.2.1 Making a decision about your recruitment or appointment, which will include receiving Personal Data from third parties such as your referees.

5.2.2 Carrying out background, reference and pre-employment health checks, where applicable.

5.2.3 Determining the terms on which you work for us.

5.2.4 Checking you are legally entitled to work in the UK.

5.2.5 Contacting you by telephone, email or text.

**5.3 Processing for the performance of a contract with you**

5.3.1 Contacting you by telephone, email or text.

5.3.2 Paying you and providing any other benefits due under the contract of employment.

5.3.3 Liaising with your pension provider.

5.3.4 Conducting performance reviews, managing performance and determining performance requirements.

5.3.5 Making decisions about salary reviews and compensation.

5.3.6 Assessing qualifications for a particular job or task, including decisions about promotions.

5.3.7 Making decisions about your continued employment or engagement.

5.3.8 Making arrangements for the termination of your employment.

5.3.9 Assessing education, training and development requirements.

5.3.10 Ascertaining your fitness to work.

5.3.11 Managing sickness and holiday absence.

**5.4 To comply with a legal obligation to which we are subject**

5.4.1 Carrying out background and reference checks, where applicable.

5.4.2 Checking you are legally entitled to work in the UK.

5.4.3 Paying you, deducting tax and National Insurance contributions and liaising with HMRC.

- 5.4.4 Complying with health and safety legislation.
- 5.4.5 Maintaining training and time management records.
- 5.5 **Where it is necessary for the purposes of our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests**
  - 5.5.1 Business management and planning, including accounting and auditing.
  - 5.5.2 Implementing HR employee relations policies and procedures.
  - 5.5.3 Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
  - 5.5.4 Preventing fraud and other crime.
  - 5.5.5 Monitoring content and use of our information and communication systems to ensure compliance with our IT policies.
  - 5.5.6 Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
  - 5.5.7 Using photographs in connection with security.
- 5.6 **The Processing is with your consent, which can be withdrawn at any time**
  - 5.6.1 Using photographs to publicise the work of Hailsham House and providing information to residents, volunteers and supporters.

## **6. IF YOU FAIL TO PROVIDE PERSONAL DATA**

- 6.1 If you fail to provide information when requested during the application process, e.g. references, it is unlikely that we will be able to take your application further.
- 6.2 Failure to provide information when you work for us may prevent us from performing the contract with you in accordance with its terms. We will tell you about the implications of not providing the information to us.

## **7. HOW WE USE SENSITIVE PERSONAL DATA**

- 7.1 We will use your sensitive Personal Data in the following circumstances:
  - 7.1.1 In limited circumstances, with your explicit written consent.
  - 7.1.2 Where we need to carry out our legal obligations or exercise our rights in connection with employment law.
  - 7.1.3 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 and reporting.

- 7.1.4 We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- 7.1.5 We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate adjustments in the workplace (or during the recruitment process, e.g. for a test or interview), to monitor and manage sickness absence and to administer benefits.
- 7.1.6 Certain roles require a high degree of integrity since they involve dealing with vulnerable residents and so we may require disclosure of your criminal records history. We will use any information that you disclose to us or that is revealed by a check with the Disclosure and Barring Service to consider your application for employment. If your application is successful, we will record that we have made the check but not the details of any convictions. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.
- 7.1.7 Less commonly, we may Process sensitive Personal Data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent.

## **8. CONSENT**

- 8.1 Some types of Processing require your consent to allow us to do them. If you have ever given your consent to a specific Processing after we have requested it, you can withdraw that consent at any time.
- 8.2 For example, if you are a candidate for a role, you provided consent to our processing your Personal Data for the purposes of the recruitment exercise. You have the right to withdraw that consent at any time. To withdraw your consent, please contact our DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely.

Similarly, if you notify us that you wish to withdraw your consent for a particular Processing while you work for us, we will no longer Process your Personal Data for that purpose or purposes.

- 8.3 Please note that the withdrawal of consent will not affect the lawfulness of any Processing before you withdrew your consent.

## **9. SHARING YOUR PERSONAL DATA**

- 9.1 **Why might you share my Personal Data with third parties?**

We will share your Personal Data with third parties where required by law (e.g. HMRC, CQC, CCG, HSE, Environmental Health, NMDS and the Police), where it is necessary to process your application or administer the working relationship with you or where we have another legitimate interest in doing so (e.g. safeguarding our residents).

## **9.2 Which third-party service providers Process my Personal Data?**

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities may also be carried out by third-party service providers: storing your data on an online portal, payroll, pension administration, benefits provision and administration and IT services.

## **9.3 How secure is my information with third-party service providers?**

All our third-party service providers are required to take appropriate security measures to protect your Personal Data 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.

## **9.4 What about other third parties?**

We may share your Personal Data with other third parties. For example, your contact details and the vacancy for which you applied are passed to your referees. The Disclosure and Barring Service (DBS) Application Form is sent to the Disclosure and Barring Service. Your information may be shared with regulators such as the CQC, CCG, HSE, Environmental Health, NMDS and the Police.

## **10. DATA RETENTION**

10.1 If your application to work for us is unsuccessful, we will retain your records for seven months after notifying you. If we wish to retain your personal information on file, on the basis that a further opportunity may arise in the future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

10.2 If your application is successful, we will retain your employment records for seven years after employment ceases and pension records for ten years after the benefit ceases.

## **11. YOUR RIGHTS IN CONNECTION WITH PERSONAL DATA**

11.1 Under certain circumstances, by law you have the right to:

11.1.1 Request access to your Personal Data (commonly known as a "data subject access request"). This enables you to receive a copy of the Personal Data we hold about you and to check that we are lawfully Processing it.

11.1.2 Request correction of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- 11.1.3 Request erasure of your Personal Data. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to Process it. You also have the right to ask us to delete or remove your Personal Data where you have exercised your right to object to Processing (see below).
- 11.1.4 Object to Processing of your Personal Data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to Processing on this ground. You also have the right to object where we are Processing your Personal Data for direct marketing purposes.
- 11.1.5 Request the restriction of Processing of your Personal Data. This enables you to ask us to suspend the Processing of Personal Data about you, for example if you want us to establish its accuracy or the reason for Processing it.
- 11.1.6 Request the transfer of your Personal Data to another party.

If you want to review, verify, correct or request erasure of your Personal Data, object to the Processing of your Personal Data, or request that we transfer a copy of your Personal Data to another party, please contact us in writing.

## **12. DATA PROTECTION OFFICER**

- 12.1 If you have any questions about this privacy notice or how we handle your Personal Data, please contact the DPO by writing to The Data Protection Officer, 20 Cranley Road, Hersham, Walton on Thames, Surrey, KT12 5BP or by email at [will@grahamcare.co.uk](mailto:will@grahamcare.co.uk).
- 12.2 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (email: <https://ico.org.uk/global/contact-us/email>; post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; telephone: 0303 123 1113).