Staff Privacy Notice

Document Reference	0841
Version No	V1
EMT Lead	Karen Tyrell, Executive Director
Author(s)	Tori Jones, Data Protection Officer Kathryn Summerfield, Director of People David Nelthorpe, Snr Corporate Services
Ratified by	Karen Tyrell, Executive Director
Signed	Karen Tyrell, Executive Director
Date Issued	Jan 2022
Review Date	Jan 2024

Document Change Log

This document will be reviewed 24 Months or as changes in legislation dictate.

Version No	Date	Document Change
1	April 2021	New item

Equality Statement

All customers, employees and members of the public should be treated fairly and with respect, regardless of age, disability, gender, marital status, membership or no membership of a trade union, race, religion, domestic circumstances, sexual orientation, ethnic or national origin, social & employment status, HIV status, or gender re-assignment.

Introduction

Humankind processes the personal data of staff members as part of recruitment and employment requirements.

As an organisation, Humankind must be clear about what it does with personal data; and this must be presented in an honest, transparent, and easy to read way.

Under the Data Protection Act 2018 and UK GDPR, individuals have rights which must be upheld when personal data is processed. This includes a right to know why we need the information, what we are doing with it and who we are sharing it with.

It is good practice to ensure that this information is written down in a document called a Privacy Notice.

This document includes Humankind's current staff privacy notice.

Guidance to the privacy notice

This privacy notice should be available and accessible to all employees, ex-employees, agency staff, contractors, secondees and those applying to work for us.

Copies should be freely available and included as part of the recruitment and induction process.

You may use this notice to provide information to individuals who are asking about their data rights and if you have any further questions, please contact your Data Protection Officer at dpo@humankindcharity.org.uk

Relevant Documentation

Humankind policies and procedures (Cascade > Policies & Forms > Information Governance):

- 0404 Privacy and Personal Data Protection Policy
- 0405 Records, Retention & Protection Policy

External documentation (such as laws, legislation, and good practice):

- Data Protection Act 2018
- UK GDPR

Websites

http://www.ico.org.uk

Table of Contents

Staff Privacy Notice

As an employer Humankind must meet its data protection and UK GDPR obligations. We are committed to ensuring that the personal data of our employees is handled in accordance with the principles set out in UK data protection legislation.

This privacy notice tells you what to expect when Humankind collects personal information about you. It applies to all employees, ex-employees, agency staff, contractors, secondees and those applying to work for us.

However, the information we will process about you will vary depending on your specific role and personal circumstances.

Humankind is the Data Controller (we decide the purpose and means of data processing) for this information. You can contact our Data Protection Officer at DPO@humankindcharity.org.uk to query matters related to data protection.

Privacy Notice Review Period

This notice was last reviewed March 2021. It will be reviewed again in March 2022 (unless changes to processing require us to update sooner).

How We Obtain Your Information

We get information about you from the following sources:

- Directly from you.
- From an employment agency.
- From your employer if you are a secondee.
- From referees, either external or internal.
- From security clearance providers (such as the Disclosure and Barring Service).
- From Occupational Health and other health providers.
- From Pension administrators and other government departments (for example tax details from HMRC)
- From your Trade Union.
- From TUPE processes (due diligence data)
- From providers of staff benefits.
- CCTV images from our landlords or taken using our own CCTV systems.

What We Collect and Why

We process the personal data related to your employment and we use the following information to carry out the contract we have with you, provide you access to business services required for your role and to manage our human resources processes:

- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses.
- Your date of birth, gender, and national insurance number.
- A copy of your passport or similar photographic identification and /or proof of address documents.
- Marital status.
- Next of kin, emergency contacts and their contact information.
- Employment and education history including your qualifications, job application, employment references, right to work information and details of any criminal convictions that you declare.

- Location of employment (e.g., home base or office location)
- Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations.
- Security clearance details including basic checks and higher security clearance details according to your job.
- Any criminal convictions that you declare to us.
- Your responses to staff surveys if this data is not anonymised.
- Information related to your salary, pension, and loans. We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave.
- Information about your job role and your employment contract including your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working).
- Details of your time spent working and any overtime, expenses or other payments claimed.
- Details of any leave including sick leave, holidays, special leave etc.
- Pension details including membership of pension schemes (current and previous).
- Your bank account details, payroll records and tax status information.
- Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking.
- Information relating to your performance and training.
- We use this information to assess your performance, to conduct pay and grading reviews and to deal with any employer / employee related disputes. We also use it to meet the training and development needs required for your role.
- Information relating to your performance at work e.g., probation reviews, Performance and Development Reviews (PDRs/appraisals), supervision notes and promotions.
- Grievance and dignity at work matters and investigations to which you may be a party or witness.
- Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued.
- Whistleblowing concerns raised by you, or to which you may be a party or witness.
- Information related to your training history and development needs.
- Information relating to monitoring. We use this information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees.
- Information about your access to data held by us for the purposes of criminal enforcement if you are involved with this work.
- Information derived from monitoring IT acceptable use standards.
- Photos and CCTV images.
- Information relating to your health and wellbeing and other special category data.
- We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees.
- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e., Statement of Fitness for Work from your GP or hospital. This includes Covid testing status, Covid vaccination and booster status.

- Information you share with us about your lived experience, which you may share for example through recruitment or 1:1s.
- Accident records if you have an accident at work.
- Details of any desk audits, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics.

We are the data controller of all data which is stored on Humankind devices, such as the equipment we provide you with for work. This means that any personal data you store about yourself (or others) is accessible by us at any time when saved or stored on these devices. In some instances (for example hard drives) it is also possible for us to access personal data which you have deleted from these devices.

Lawful Basis

Depending on the processing activity, we rely on the following lawful basis for processing your personal data under the GDPR:

- Article 6(1)(b) which relates to processing necessary for the performance of a contract.
- Article 6(1)(c) so we can comply with our legal obligations as your employer.
- Article 6(1)(d) in order to protect your vital interests or those of another person.
- Article 6(1)(f) for the purposes of our legitimate interest.

For information about the lawful basis for processing data pertaining to your vaccination status please see the Covid 19 Vaccination Status Privacy Notice.

Special Category Data

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.

- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(j) for archiving purposes in the public interest.

In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) of the DPA 2018. These relate to the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee.

For information about the special category conditions we rely on for processing data pertaining to your vaccination status please see the Covid 19 Vaccination Status Privacy Notice.

We process information about staff criminal convictions and offences. The lawful basis we rely on to process this data are:

- Article 6(1)(e) for the performance of our public task. In addition, we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a).
- Article 6(1)(b) for the performance of a contract. In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1.

Information Sharing

In some circumstances, such as under a court order, we are legally obliged to share your personal information *(Data Protection Act 2018; Schedule 2; part 5).* An example of this is if a court requests that we disclose comparator information within an employment tribunal. Under the UK GDPR, we do not need to notify you that we have shared your data for this purpose so long as it is court ordered and necessary.

We may share information about you with HMRC for the purpose of collecting tax and national insurance contributions.

We use data processors for some of our processing activities. A list of our current data processors can be found at Appendix A. We hold contracts with processors which detail processing arrangements.

During your employment you may be referred to occupational health following a request to HR by you or your line manager. This may result in a face-to-face consultation, a telephone appointment with an occupational healthcare professional and/or a medical report from a GP or specialist. We use Care-First to provide our employee assistance programme and Everwell to provide our occupational health service. A link to their privacy notices can be found in Appendix A.

If you leave, or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference. For example, we may be asked to confirm the dates of your employment or your job role. If you are still employed by us at the time the request for a reference is received, we will discuss this with you before providing this.

We will also share information about you with our training providers. For example, this will include information such as your name, contact details and job role. When necessary, we will also share information about any dietary or access requirements that you might have when you attend training events. The main providers we work with are listed in Appendix A. Please note that on occasion, we may use a different provider for a 'one-off' training event and the details of which will not be added to the appendix A. However, you will be aware of the provider when you attend the training and the data shared will be the same as we have detailed in this paragraph.

As part of Transfer of Undertakings (Protection of Employment)/TUPE process Humankind will be asked to produce a list of job roles, as part of due diligence, which will be transferred to the new employer/organisation taking on the new contract. At the initial stage, personal data is not required to be shared. However, this data may not always be considered anonymous if the job role is held by only one person (or a very small group of persons) as by process of elimination, their identity could be determined. At the closing stages of the TUPE process the full list of names and contractual information is shared to the receiving organisation as part of the Employer Liability requirement. Information about the TUPE process and any proposed measures must be provided to employees prior to the transfer date. Please see Cascade > Policies and Forms > HR > Management of Change Policy.

Keeping Your Information Safe

Human resources/personnel data: Personal data is held on secure cloud-based system in the UK and records are maintained on separate networks with secure access.

Training data: Personal data is held on a secure cloud-based system in the UK. Records are maintained on separate networks with secure access.

How Long We Keep Your Information For

We keep your information in line with our records, retention and protection policy, the key information is in Appendix B.

Your Rights

Under the Data Protection Act 2018 and 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.
- rights in relation to automated decision making and profiling.

Please note that some of these rights only apply in certain circumstances and we may not be able to fulfil every request. Where a request is declined, we will always explain our decision in full.

To request access to your data or to contact us about any of the rights we have listed, you can email caldicott.guardian@humankindcharity.org.uk

Overseas Transfers of Data

We do not transfer staff personal data overseas unless you have requested that we send a reference overseas. In this case (and only with your consent) we would transfer the information using password protect, making you aware that once the information leaves our environment, we are not able to guarantee its security.

If you use a Humankind Zoom account as part of your role please be aware that Zoom has servers based in the USA. We have signed a Standard Contractual Clause document with Zoom. According to the General Data Protection Regulation (GDPR), contractual clauses ensure appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries.

Automated Decision Making and Profiling

We use some automated decision making and profiling when we sift job applications. We use software that can identify where mandatory fields have not been completed and which check for right to work criteria.

This is the only time we use automated decision making and profiling. Once, the initial sift has been completed by our recruitment system, a human panel is arranged who review all applications and shortlist using a scoring process related to how well the applicant has met the criteria detailed in the job description and personal specification.

How to Complain

If you are unhappy about an issue relating to your data, you should complain through your line manager who will log this on the hub (ticking the box to say that this is in the information governance issue) and follow the Humankind complaints process (see Cascade > Policies-and-Forms > Corporate > 0313 Complaints Policy Feedback and Guidance).

To make a formal complaint about the way we have processed your data you can take this to the UK's independent body set up to uphold information rights:

Information Commissioner's Officer (ICO)

0303 123 1113

http://www.ico.org.uk

Appendix A: Data Processors

Data Processor	Purpose	**Privacy Notice Link**
Everwell	Occupational Health	https://everwelloh-charm.co.uk/Terms/PrivacyPolicy
GBG	DBS checks	https://www.gbgplc.com/privacy-policy/
Taye Training	Training Provider	https://tayetraining.org.uk/privacy/
Care-First	Employee Assistance	https://www.care-first.co.uk/privacy
GP Strategies	Training Provider (apprenticeships)	https://www.gpstl-apprenticeships.co.uk/legal-information/privacy-policy.shtml
Teesside University	University Training Provider (apprenticeships)	https://www.tees.ac.uk/sections/about/public_information/copyright.cfm?display=privacy
East Durham College	College Training Provider (apprenticeships)	https://www.eastdurham.ac.uk/cookie_privacy_policy
Newcastle & Staffordshire Colleges Group	College Training Provider (apprenticeships)	https://nscg.ac.uk/privacy-policy
Learning Curve	Training Provider (apprenticeships)	https://www.learningcurvegroup.co.uk/privacy
DAS	Government website (apprenticeship personal details)	https://accounts.manage-apprenticeships.service.gov.uk/service/privacy
HIT Training Ltd	Training Provider (apprenticeships)	https://hittraining.co.uk/sites/default/files/website-privacy-policy_0.pdf
Open University	University Training Provider (apprenticeships)	http://www.open.ac.uk/about/main/strategy-and-policies/policies-and-statements/website-privacy-ou
New College Durham	College Training Provider (apprenticeships)	https://www.newcollegedurham.ac.uk/privacynotices/
Darlington College	College Training Provider (apprenticeships)	https://darlington.ac.uk/privacy-policy/
Bromley College of Further & Higher Education (part of London South East Colleges):	College Training Provider (apprenticeships)	https://www.educations.com/privacy-policy/

Appendix B: Retention Periods Relevant to Staff

Document or data type	Retention period
Personal Files	6 years after employment ceases
Right to Work ID	2 years after employment ceases
Payroll Information	6 years after employment ceases
Pension Information	7 years after employment ceases
Applications of Unsuccessful Job Candidates	6 months from application
Occupational Health Files	6 years after employment ceases
Covid Status	6 years after employment ceases
Covid Vaccination Status	1 year after employment ceases
Learning and Development Records	6 years after employment ceases
Whistleblowing Documentation	6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data is removed immediately.
Working Time Records	2 years since the date they were made
Records in relation to hours worked and payments made to workers	3 years
Statutory Maternity, Shared Parental, Paternity and Adoption Pay Records	3 years from the end of the tax year in which the maternity/paternity period ends
Pay as You Earn (PAYE) Records and HMRC Correspondence	3 years from the end of the tax year in which they relate to
Parental leave information	5 years from birth/adoption (or 18 years if the child is disabled).
Statutory Sick Pay records	3 years from the end of the tax year they relate to
Annual return of employees and directors' expenses and benefits (P11D)	3 years from the end of the tax year they relate to
Accident reports and any evidence collected as part of investigation into the accident (ensuing from obligation on an employer to retain records of any reportable accident, reportable diagnosis, death, or injury in connection with work)	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). Where litigation and insurance claims apply retention to extend based on legal guidance.
CCTV	On premises where CCTV is installed, footage is automatically wiped by the system. This varies for each system but is generally wiped every 1 week or every 1 month. For details on a specific system, you can email caldicott.guardian@humankindcharity.org.uk

Staff surveys	Survey questions blend both quantitative and qualitative responses and some free text boxes are included. Anonymity is offered and we advise you not to share identifiable information about yourself in these boxes if you wish to remain anonymous. We keep this as long as it is necessary and as described on the survey.
Equal Opportunities Monitoring Information	This is done via the PeopleKind HR database system for our workforce. For new recruits this is captured via the application process and retained for 6 months if they are not successful at interview. For successful candidates, this data is transferred onto the PeopleKind HR database.
Staff ID Badges	Duration of employment. This is destroyed as part of the exit procedure.