

## Employee Privacy Notice

Version 2.0. Last reviewed 25<sup>th</sup> July 2023.

### 1. Introduction

1.1 This Privacy Notice describes how your personal information is processed and protected as an employee of The Housing Plus Group Limited or one of its subsidiaries and informs you of your individual rights in relation to personal data.

1.2 The Housing Plus Group Limited ("the Group") is registered in England and Wales as a Charitable Community Benefit Society (30224R) and as a Data Controller with the Information Commissioner's Office (ICO) (Z1210914). Our registered office is located at Acton Court, Acton Gate, Stafford ST18 9AP.

### 2. What information does the Group collect?

2.1 The Group collects and processes a range of information about you. This includes:

2.1.1 your name, address, contact details and image, including your personal email address and telephone number, data of birth and gender, including proof of these, for example copies of utility bills, passport, birth certificate, and/or drivers licence;

2.1.2 the terms and conditions of your employment/appointment, including details of other roles you hold if you are a non-executive director;

2.1.3 details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Group or its subsidiaries;

2.1.4 information about your remuneration, including entitlement to benefits such as pensions or insurance cover, annual leave, hours of work and attendance at work;

2.1.5 details of your bank account and national insurance number;

2.1.6 information about your marital status, next of kin, dependants and emergency contacts;

2.1.7 information about your nationality and entitlement to work in the UK;

2.1.8 information about your criminal record (in accordance with the Rehabilitation of Offenders Act 1974);

2.1.9 details of your learning and development record;

2.1.10 details of periods of leave taken by you, including holiday, sickness absence, unpaid leave and sabbaticals, and the reasons for the leave;

2.1.11 details of disciplinary or grievance procedures in which you have been involved, including any warnings issues to you and related correspondence;

- 2.1.12 details of conflicts of interest;
- 2.1.13 assessments of your performance, including appraisals, performance reviews and rating, performance improvement plans and related correspondence;
- 2.1.14 information about medical or health conditions, including whether or not you have a disability for which the Group needs to make reasonable adjustments and provide support;
- 2.1.15 equal opportunities monitoring information including information about your ethnic origin, sexual orientation, health, religion or belief;
- 2.1.16 details of your trade union membership;
- 2.1.17 information about the vehicle you drive for the purposes of work, including details of your car insurance, vehicle details, and MOT;
- 2.1.18 personal information (for example location information) collected incidentally by services installed on company-issued devices or by the nature of the device and/or networking equipment you are connected to (for example, a personal device connected to the Groups guest WiFi). This type of processing may reveal patterns of life or personal information (for example, the connection/disconnection of a device from WiFi may reveal your pattern of work at a particular location);
- 2.1.19 personal information captured for monitoring, security and health and safety purposes, including but not limited to, GPS trackers, tachograph data and other position and time-based derived data, and data captured in the Groups legitimate interest to protect the security of systems and network infrastructure. This information may reveal patterns of life (for example, the hours you utilise a company-issued device);
- 2.1.20 personal information you upload or share via company devices, systems, and infrastructure, for example (but not limited to), email sent to or from a company email address, messages sent from a company-issued mobile phone, including WhatsApp.

### **3. How does the Group collect this data?**

- 3.1 The Group collects your personal information in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.
- 3.2 In some cases, the Group may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal

records checks permitted by law. The Group may also seek information from third parties such as GPs but with your consent only.

3.3 The Group operates a number of different systems, processes, and procedures designed to protect the IT network and infrastructure and the data processed by those systems. For example (but not limited to), these systems may capture personal information at the point of creation (e.g., a file is created) or during transmission (e.g., an email is sent).

3.4 Data will be stored in a range of different places, including but not limited to, human resource systems, your personnel file, and in other IT systems (including the email and file systems such as 'Microsoft Exchange' and 'Microsoft SharePoint').

#### **4. Why does the Group process your personal data?**

4.1 The Group needs to process your personal data in order to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

4.2 In some cases, the Group needs to process data to ensure that it is complying with its legal obligations. For example, it is a legal requirement that we check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

4.3 In other cases, the Group has a legitimate interest to process personal data before, during and after the end of the employment relationship. Where the Group relies on legitimate interest the rights and freedoms of the data subject have been assessed to ensure the protection of those rights and freedoms.

4.4 Processing employee data allows the Group to:

4.4.1 run recruitment, onboarding and promotion processes;

4.4.2 maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights, and to issue you with an ID card;

4.4.3 operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace, including conducting different types of investigations (e.g., health and safety and disciplinary);

4.4.4 operate and keep a record of employee performance and related processes including 1-to-1s and reviews, to foster and plan for career development, and for succession planning and workforce management purposes;

4.4.5 operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;

- 4.4.6 obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
  - 4.4.7 operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the firm complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
  - 4.4.8 ensure effective general HR and business administration;
  - 4.4.9 provide references on request for current or former employees;
  - 4.4.10 respond to and defend against legal claims, including potential claims;
  - 4.4.11 respond to requests for information form, and support investigations by, enforcement agencies, including but not limited to, the Police, National Crime Agency, Health and Safety Executive (HSE), Fire Authority, and Local Authority (where they act as health and safety enforcement agencies);
  - 4.4.12 maintain and promote equality in the workplace;
  - 4.4.13 create and disseminate promotional materials including photos, videos and written media in order to advertise, promote and inform existing and potential customers and employees of the services and activities of the Group;
  - 4.4.14 communicate with staff via their personal email address to keep employees apprised of news, changes and information, and to gather information through the use of staff surveys; and
  - 4.4.15 maintain details of employee learning and development records.
- 4.5 Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities). Where we handle your personal data in relation to health, we endeavour to do so with your consent.
- 4.6 Where the firm processes special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring, which is a regulatory requirement. The information collected and analysed for regulatory reporting is done so on an anonymous basis.

## **5. Who has access to this data?**

- 5.1 Your personal information (including special category data) may be shared (where necessary) internally, with the following teams; Human Resources (People Team),

Finance (including payroll), IT, Legal (including audit and data protection) and your line manager, managers in the business area in which you work and the senior management team.

- 5.2 Access to your data is considered necessary, if it is a requirement for legal, regulatory or compliance purposes (for example, supplying personal information to the HSE or the Local Authority for health and safety investigations), audit purposes (for example as evidence of certain activities or functions) or enables a person to perform activities in relation to their role. This may include accessing your company issued devices (e.g., laptop, phone, tablet) in the event of an investigation.
- 5.3 Access to personal data is limited only to that information which is necessary and required to conduct an activity. For example, if a complaint is made, different teams will need to work together to view and report on documentation, to enable the investigation and resolution of that complaint.
- 5.4 The Group shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.
- 5.5 The Group also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits including pensions and the provision of occupational health services and operation of Early Intervention Service (EIS) (see Appendix 1).
- 5.6 The Group reserves the right to share your personal data in accordance with legal requirements where an employee is under investigation and/or the information is requested by a law enforcement entity (for example, the Police).
- 5.7 Other sharing and transfers of your personal information may occur where you have authorised or asked us to do so with your consent.

## **6. International Transfers**

- 6.1 The Group does not routinely conduct international transfers of personal data. However, due to the international nature of the internet and the products and services the Group utilises, your personal data may be transferred outside of the United Kingdom (UK) and European Economic Area (EEA). For example, where staff use WhatsApp to communicate with customers via their work-issued mobile device, location data may be sent to the United States of America (USA).
- 6.2 Where international transfers of personal information do occur, they will be conducted in accordance with the Data Protection Act 2018 and UK General Data Protection Regulation.

## **7. How does the Group protect this data?**

- 7.1 The Group takes the security of your personal data seriously. The Group has organisational and technical methods in place to ensure the security of its data. This

includes training, internal documentation (such as policies, procedures, and guidance), firewalls, network monitoring, intrusion prevention systems, and data loss prevention, among others. These controls ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by the Groups employees in the performance of their duties. The majority of your personal data, including special category data, is stored within human resource systems.

7.2 Where the firm engages third parties to process personal data on its behalf, they do so, on the basis of written instructions; are under a duty of confidentiality and are obliged to implement appropriate technical and firm wide measures to ensure the security of data.

## **8. How long does the Group keep this data?**

8.1 The Group will hold your personal data for the duration of your employment. The periods for which your data is held can be obtained by referring to the table in Appendix 2 or the Group's data retention schedule. Personal data is destroyed at regular intervals to ensure personal information is only retained for as long as it is required.

## **9. Your rights**

9.1 As a data subject, you have a number of rights. You can:

9.1.1 access and obtain a copy of your data on request;

9.1.2 require the Group to change incorrect or incomplete data;

9.1.3 ask the Group to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;

9.1.4 object to the processing of your data where the firm is relying on its legitimate interests as the legal ground for processing; and

9.1.5 withdraw consent. Where you have provided your consent for personal data processing you can withdraw consent at any time.

9.2 If you would like to exercise any of these rights, please contact the Data Protection Team at [data.protection@housingplusgroup.co.uk](mailto:data.protection@housingplusgroup.co.uk), or where matters require escalation, the Data Protection Officer, Irene Molyneux, Director of Legal and Governance.

9.3 If you believe that the Group has not complied with your data protection rights or has processed your personal data unlawfully, you can formally make a complaint to the Information Commissioner's Office (ICO). You can visit the Commissioner's website at [www.ico.org.uk](http://www.ico.org.uk) to learn more or you can phone the ICO on 0303 123 1113.

## **10. What if you do not provide personal data?**

10.1 You have some obligations under your employment contract to provide the Group with personal data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied

duty of good faith. You may also have to provide the Group with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

- 10.2 Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the Group to enter a contract of employment with you. If you do not provide other information, this will hinder the Group's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

## 11. Automated Decision-making

- 11.1 Employee personal information is not subject to automated decision-making.

## 12. Questions and Complaints

- 12.1 If you have questions after reading this privacy policy, you can get in touch with the Group's Data Protection Officer using the contact details below.
- 12.2 In certain circumstances, you can complain to the Information Commissioner's Office (ICO) about the use of your personal data. You can find out more information about data protection at [www.ico.org.uk](http://www.ico.org.uk) and you can find further contact details below to gain independent advice from the ICO.

## 13. The Data Protection Officer

The Group has a Data Protection Officer (DPO) who monitors compliance and advises the Group on data protection, privacy, and the security of personal data.

Data Protection Officer  
Housing Plus Group  
Acton Court,  
Acton Gate,  
Stafford,  
ST18 9AP

Email: [data.protection@housingplusgroup.co.uk](mailto:data.protection@housingplusgroup.co.uk)  
Customer services: 0800 048 8955

## 14. Information Commissioner's Office

For independent advice about data protection and/or to raise concerns about the use of personal data you can contact the Information Commissioner's Office (ICO).

Information Commissioner's Office  
Wycliffe House,  
Water Lane,  
Wilmslow,  
Cheshire,  
SK9 5AF

Phone: 0303 123 1113  
 Email: casework@ico.org.uk  
 Website: www.ico.org.uk

## 15. Glossary

Term	Definition
Company-owned device	An electronic device owned by the Housing Plus Group Limited or any of its subsidiaries.
Data Controller	An entity which alone, or jointly with others, determines the purposes and means of the processing of personal data.
Personal data / information	Any information relating to a person who can be identified, directly or indirectly, by reference to an identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identity of that person.
Personal device	An electronic device owned by an individual.
Processing	In relation to personal data, means any operation or set of operations which is performed on personal data or sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction).
Sabbatical	A period of paid or unpaid time away from work agreed between an employer and employee.
Subsidiary	A company owned by another company.

## 16. Document changes

Version	Description	Date
2.0	Document released	25/07/23



## Appendix 1: Third party data sharing

Appendix 1 contains a list of the most common third parties employee data may be shared with, dependant on the particular activity concerned. This list may not be exhaustive at the time of reading. The list is updated at each review of this document. You can contact the People Team to gain an up to date version at [hr@housingplusgroup.co.uk](mailto:hr@housingplusgroup.co.uk).

Processor	Reason
ACAS (Advisory, Conciliation, and Arbitration Service)	Employee relations and dispute resolution
Access UK Ltd	Human Resources Management System
Alphabet Inc	Google web analytics
AXA Insurance UK Plc	Insurance provision
Beevers and Struthers	Internal auditors
Best Companies Limited	Employee surveys and data analysis
Canada Life Limited	Health insurance and income protection
Care Quality Commission (CQC)	National health care regulator
Careskills Academy Ltd	People development academy
Civica UK Limited	Human Resources Management System
Disclosure and Barring Service	Background and criminal record checks
DWF Group Plc	Legal firm
Fire Authority	Health and safety investigations
First Actuarial LLP	Law firm, pensions
GreatWithTalent Ltd	Training and development
Health and Safety Executive (HSE)	National health and safety regulator
HMRC	Legal obligation
Housing Ombudsman Service	Regulator investigations
Information Commissioner's Office (ICO)	National data protection supervisory authority
JMW Solicitors LLP	Overseas recruitment
KPMG	Settlement information and audit

Learning Pool Limited	People development academy
License Check Ltd	Vehicle license, MOT, and car insurance check
MailChimp (Inuit Inc)	Email newsletters
Mercer LLC	Insurance
Microsoft Corporation	Outlook, SharePoint, OneDrive, Teams
MRI Software LLC	Documotive document management system
National Employment Saving Trust (NEST)	Pensions
Nursing and Midwifery Council (NWC)	National regulator of nurses and midwives
Octopus Energy	Electric vehicle scheme management
Phoenix Occupational Health Ltd	Occupational health assessment
Restore Datashred Limited	Information destruction
Scottish Widows Limited	Pension provision
ShredPro Limited	Information destruction
Shred-It Limited	Information destruction
Local Government Pension Schemes	Pension provision

## Appendix 2: Data retention periods

Type of data	Description	Related legislation or best practice	Retention period
Recruitment	Records application details for roles within the organisation, medical, disability and reference checks as part of the recruitment process, and the contract of employment.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Non-executive director personal details	Records required for the Register of Directors, and Board Member Deed of Agreement for Service.	Companies Act 2006.	Indefinitely for Register of Directors, and 12 years from date of appointment
Pay and benefits	Records payroll and salary records, including benefits which an employee receives.	Taxes Management Act 1970.	Length of employment plus 6 years.
Income tax and NI records	Records relating to income tax and national insurance (NI) returns, income tax records, and correspondence with HMRC.	The Income Tax (Employments) Regulations 1993	Not less than 3 years after the end of the relevant financial year.
Minimum Wage Records	Records relating to the national minimum wage.	National Minimum Wage Act 1998	3 years after the end of the pay reference periods following the one that the records cover.
Driving Checks	Records of employees driving checks to ensure drivers can operate a vehicle for work	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.

DBS	DBS record reference, date, level of DBS, and date of expiry. Only information required to obtain DBS retained. This information is subject to a renewal every 3 years.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Terms and Conditions of Employment	Records of contractual information including conditions, offers, variations and particulars.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Employee Relations Data	Records of cases for disciplinary, grievance, capability, management concerns, and change management.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years. Case files retained for period of the warning, then only outcome letter retained.
Sickness and Wellbeing	Sickness absence case information, records relating to employee health and wellbeing.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Maternity/Paternity/Adoption/ Shared parental leave/ Flexible working	Records relating to employee maternity, paternity, adoption or parental leave.	The Statutory Maternity Pay (General) Regulations 1986 as amended, Maternity & Parental Leave Regulations 1999.	Length of employment plus 6 years.
Regular Reviews/1-2-1's/Performance data	Records of employee personal development discussions (1-2-1 and regular reviews), performance development (skills matrices/PDP's) and training	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Leavers	Records relating to leavers and employment termination	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.

Training/Development	Records of personal and professional qualifications, coaching sessions, company approved training and financial support.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years. HAVS and Asbestos training records retained indefinitely from April 2019.
First Aid and Fire Warden Training	Records relating to first aid and fire warden training.	Health and Safety (First Aid) Regulations 1981, and Fire Precautions (Workplace) Regulations 1997.	Length of employment plus 6 years.
Asbestos and Lead records	Medical records and details relating to Lead and Asbestos.	The Control of Asbestos at Work Regulations 2002, 2006 and 2012, and The Control of Lead at Work Regulations 1998 as amended by the Control of Lead at Work Regulations 2022	40 years from the date of last entry.
Subject Access Request	The content of subject access requests.	Data Protection Act 2018	2 years for the content of the request, 6 years for information relating to the request.
Early Careers (Apprentices and Graduates)	Records of levy payments, apprenticeship and graduate qualifications tracking.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Employee Engagement	Information relating to employee feedback and surveys	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.

Pension records	Information relating to pension and retirement benefits schemes.	The Retirement Benefits Schemes (Information Powers) Regulation 1995.	Length of employment plus 15 years.
Furlough	Contractual terms and conditions relating to the COVID-19 pandemic.	Former statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'.	Length of employment plus 6 years.
Clinically Extremely Vulnerable Groups	Information relating to those individuals who were required to shield as part of the COVID-19 pandemic.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
COVID-19 Vaccination Status	Information shared relating to COVID-19 vaccination status.	Chartered Institute for Personnel and Development (CIPD) HR records retention best practice.	Length of employment plus 6 years.
Whistleblowing documents		Public Interest Disclosure Act 1998	6 months following the outcome (if substantiated) otherwise personal data removed immediately.