Employee Privacy Notice

As employers we must meet contractual, statutory, and administrative obligations. We are committed to ensuring that the personal data of employees is handled in accordance with the principles set out in Data Protection Law. This privacy notice tells you what to expect when We collect personal information about you. It applies to all employees, ex-employees, agency staff, contractors, and non-executive directors. However, the information We process will vary depending on your specific role and personal circumstances.

Aspire Housing Employees

Aspire Housing is the data controller and is registered with the Information Commissioner (registration number Z7678641). Parts of this notice refer to our other corporate policies and procedures.

Contacting Us

Our Registered Office is Aspire Housing, Kingsley, The Brampton, Newcastle-under-Lyme, ST5 0QW Telephone: 01782 635200. The Data Protection Officer for all data controllers in the group can be contacted using the above information or by email; DPO@aspirehousing.co.uk.

In this notice.

- How We get your information
- What personal data We process and why
- Lawful basis for processing your personal data
- How long We keep your personal data
- Data sharing
- Do we use any data processors
- Transfers of personal data
- Further information
- Your rights in relation to this processing

How do we get your information?

We get information about you from the following sources:

- Directly from you.
- From other employees, including your manager.
- From an employment agency.
- From referees, either external or internal.
- From security clearance providers.
- 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 providers of staff benefits.
- Images from our CCTV systems.

What personal data we process and why

Information related to your employment **contract (UK GDPR article 6(1)(b)).**
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 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 NI 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.
• Details of any secondary employment, conflict of interest declarations or gift declarations.
• 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 have a **legal obligation (UK GDPR article 6(1)(c))** to 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 finish 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, including overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets.
• Details of any leave including sick leave, holidays, special leave etc.
• Pension details including membership of both state and occupational pension schemes (both current and previous).
• Your bank account details, payroll records and tax status information.
• Trade Union membership for the purpose of the deduction of subscriptions directly from salary.
• 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 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.
• 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 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.

Legitimate Interests (UK GDPR Article 6(1)(f))

1) **Information relating to your performance and training**.
We have a **legitimate Interest** to process 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, 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.

2) **Car parking spaces** to allocate spaces safely and appropriately.
If you are allocated a car parking space our facilities department also hold vehicle licence plate details linked to you. These details are deleted when staff leave.

3) **Monitoring of staff** to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees. All our IT systems, and the swipe access system for the entry and exit of our premises are auditable and can be monitored, though we don't do so routinely.

If you drive, or travel in, a company owned Maintenance Team vehicle, its movements will be tracked for insurance and safety purposes. Your driving style will be recorded and will be reported if there is a reason to suspect unlawful driving, or where there is a possible insurance claim. We use a specialist firm to provide this service under a written agreement.

We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our IT systems, equipment & vehicles. However, we reserve the right to log and monitor such use in line with our Information Security & Systems Usage Policy. Any targeted monitoring of staff related to the above will take place within the context of our disciplinary procedures.

If you operate as a lone-worker, you will install the StaySafe App on your phone. This App monitors your location and movements. It allows you to raise an alarm to protect your safety or automatically raises an alarm after prolonged non-movement. We use a specialist firm to provide this service under a written agreement.

4) **Security passes** to maintain security.
All staff are all issued with a security pass that displays their name, department, staff reference number and photograph. Staff pass details (names, numbers and photographs) are held on a machine controlled by Facilities and can only be accessed by a restricted number of

5) **CCTV** to maintain security, prevent and record crime and anti-social behaviour.
We operate CCTV in the car parks, grounds and inside our premises to monitor access to certain areas of the office. Further information is available in our CCTV policy.

6) **Occupational health,** as an employer it is in our interest to offer this service.
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 PAM Occupational Health to provide our occupational health service and who may be the data controller for your information. The information you provide will be held by PAM, who will give us a fit to work certificate or a report with recommendations. You can read PAM's privacy notice here - PAM Group

7) **Staff Development and Planning**, it is in our interest as an employer to carry this out.
Our Learning & Development department use online learning platforms for the facilitation of its work-related courses. 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.

8) Green Car Scheme, we offer this scheme as an employer.
If you take part in this scheme, we will share your information with the scheme provider limited to the minimum required.

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. We have an Appropriate Policy Document as required by The Data Protection Act 2018, Schedule 1, for this processing.
• 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)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
• Article 9(2)(f) for the establishment, exercise, or defence of legal claims.

Criminal convictions and offences
We process information about staff criminal convictions and offences. The lawful basis we rely on to process this data are:
• Article 6(1)(b) for the performance of a contract and Article 9(2)(b), exercising our rights as an employer

How long we keep your personal data
We retain data relating to your employment for 6 years beyond the end your contract, except where we have a legal obligation to hold it for longer. For more information about how long we hold your personal data, see our retention schedule.

Data Sharing
We will share information about you with third parties including government agencies, pension providers and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions. In some circumstances, such as under a court order, we are legally obliged to share information. We will only ever share the minimum required and in a secure manner.

Trade Union Membership
The Trade Unions are controllers for the personal information connected to your union membership. Aspire holds some union subscription details in order to process salary deductions for union membership for which you will have given your consent.

Do we use any data processors?
Where we use Data Processors, we have a written agreement with them that ensures your data is protected and secure.
We use several data processors to store employment and payroll data, track vehicles and operate CCTV.

Transfers of personal data
We don't routinely transfer staff personal data overseas but when this is necessary, we ensure that we have appropriate safeguards in place.

Further information
Whistle-blowers
Aspire has a policy and procedure in place to enable its current staff and ex-employees to have an avenue for raising concerns about malpractice. If you wish to raise a concern, please refer to the whistleblowing policy. Although every effort will be taken to restrict the processing of your personal data and maintain

confidentiality whether this is possible will be dependent on the nature of the concern and any resulting investigation.

Equal opportunities monitoring

Equal opportunities information provided by job applicants is attached to the relevant application on our applicant tracking system when you apply for a role at Aspire.
This information is not made available to any staff outside our recruitment team (including hiring managers) in a way which can identify you. This information is anonymised after six months and retained for reporting purposes only.

Requests for references

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.

Your Data Protection Rights

Under data protection law you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

1. The **right to access** the personal data we hold about you. This is known as a 'subject access request' (SAR). This right always applies. There are some exemptions, which means you may not always receive all the information we process. We have one calendar month to provide you with the information you have asked for, although this may be extended to two months where requests are complex.

Personnel files. Physical, and electronic records are held for each member of staff. Data is held securely on our systems and at our premises. You can request your personnel file by emailing the HR team or by submitting an access request to DPO@aspirehousing.co.uk You can also make a verbal request for your information. You will not be able to take away your physical file. Your request will be handled outside the case management area with restricted access. We will consult internally with members of staff who might hold personal data about you.

2. The **right to have the information rectified** if it is inaccurate or incomplete. This right always applies.

3. In certain circumstances you have the **right to have your information erased** from our records. You can do this where;

- the information is no longer necessary in relation to the purpose for which we originally collected/processed it
- you withdraw consent.
- you object to the processing and there is no overriding legitimate interest for us continuing the processing.
- we unlawfully processed the information.
- the personal information has to be erased in order to comply with a legal obligation.

We can refuse to erase your personal information where the personal information is processed for the following reasons:

to exercise the right of freedom of expression and information

- to enable functions designed to protect the public to be achieved e.g. government or regulatory functions.
-

- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes
- the exercise or defence of legal claims; or
- where we have an overriding legitimate interest for continuing with the processing

4. The **right to object to processing** where we say it is in our legitimate interests. We must stop using the information unless we can show there is a compelling legitimate reason for the processing, which override your interests and rights, or the processing is necessary for us, or someone else to bring or defend legal claims.

5. You have the **right to require us to stop processing** your personal information. When processing is restricted, we can store the information, but not do anything with it. You can do this where:

- You challenge the accuracy of the information (we must restrict processing until we have verified its accuracy).
- You challenge whether we have a legitimate interest in using the information.
- If the processing is a breach of the GDPR or otherwise unlawful
- If we no longer need the personal data but you need the information to establish, exercise or defend a legal claim.

If we have disclosed your personal information to third parties, we must inform them about the restriction on processing, unless it is impossible or involves disproportionate effort to do so.

6. Your **right to data portability**. This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organization to another or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated.

7. The **right to complain** to us and/or to the Information Commissioner's Office if your information is being used unlawfully (contact details are below).

8. The **right to challenge any automated decision making** or profiling that may be carried out using your information.

If you would like to contact us about your data protection rights, please contact:

The Data Protection Officer, Aspire Housing, Kingsley, The Brampton, Newcastle-under-Lyme, ST5 0QW. Telephone: 01782 635200. Email: DPO@aspirehousing.co.uk

If you have queries or concerns about how we have processed your information you can complain to our Data Protection Officer. If you remain di-satisfied you can complain to the Information Commissioners Office the contact details are as follows: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. https://ico.org.uk