

# Employee and Applicant Privacy Notice – How we use Your Personal Information



As an employee, or job applicant Clarion Housing Group (Clarion) needs to process personal data about you in order to deliver employment related services.

We are committed to treating your information securely, with respect and in line with data protection law.

This privacy notice tells you what to expect when the Clarion Housing Group (CHG) processes your personal data. 'Processing' is a broad term covering actions taken with your information from the point of collection through to the point of secure destruction and everything in between for example: using it, storing it, updating or amending it and sharing it.

Clarion Housing Group includes a number of subsidiary organisations including Clarion Housing Association, Clarion Response, Grange, Latimer and Clarion Futures. We are all responsible to you. Please see the Clarion Housing Group Website for our [registered company information](#), including registration details and registered offices of all the entities associated with Clarion.

This privacy notice is regularly reviewed and whilst we recommend that you keep up to date via the intranet (or Workday site for job applicants), any major changes will be brought to your attention.

## 1. Who does this notice apply to?

This notice applies to prospective employees (job applicants), former employees and all employees working *for* or *with* CHG or any of its subsidiaries, including contractors, consultants, casual workers and volunteers.

## 2. What information do we collect and how is this used?

When we ask you for information, we will only collect relevant information and we will make it clear why we need it and when provision of the information is optional.

Most information we hold will be collected from you but where needed, we will also obtain this from third parties such as recruitment agencies, past employers and medical professionals (in the case of occupational health). Where required, we will seek your permission to process information from third parties.

At times, Clarion also obtains information from publicly accessible sources and engages the services of market research organisations to validate, or where appropriate, enhance the information that we hold.

We collect and process information (as applicable):

- During the application and recruitment process including verification of eligibility, references and qualifications:
  - We will need your name and contact details (home address; personal email address; contact telephone numbers; emergency contact details)
  - CVs and/or applications, references and interview notes
  - DBS (Disclosure & Barring service) information in connection with roles subject to a satisfactory criminal records check
  - Letters of offer and acceptance of employment
  - Establishing a contact point in the event of an emergency (such as next of kin)

Provision of personal information is a 'contractual requirement' meaning that without this information we will be unable to offer you a role at Clarion. It will be made clear at the point of data collection whether any information is optional at this stage. Please contact us if you have any queries. (Also see section 3 for further information about special category data)

At times, Clarion will also be under a legal obligation to process this information, for example where we are required to take a copy of your passport (and / or other suitable documents) to check your eligibility to work in the UK.

- During the course of your employment and once your employment has ended (as relevant / necessary) for example:
  - We will need a photo for use on your employee photo ID badge/card
  - Managing your employment. This will include the information you have provided as well as information contributed by others about you, for example, performance reviews and development plans, probation assessments, 1:1 meeting notes and assessments, training records and development needs, photographs and videos (e.g. intranet profile pictures)
  - Dealing with disciplinary matters, grievances and employment tribunals
  - Administering pay, pensions and other benefits. This will include salary and benefit information; payroll information (bank details, tax code, national insurance number and details of any deductions such as a season ticket loan)
  - Monitoring reasonable adjustments and absences including annual leave, sickness absence and compassionate leave. (This will include medical and occupational health information where relevant)
  - DBS (Disclosure & Barring service) information in connection with roles subject to a satisfactory criminal records check

- Exit interviews at the end of your employment

The provision and processing of personal information is a contractual requirement (also see section 3 for further information about the special category data). This means that without this information we will be unable to provide employment services to you. For example, if you do not provide us with your bank details, we are unable to pay you. We will always make it clear when the provision of data is optional. If you have any queries, please contact us.

- Publication of personal data (including photos/images/case studies) relating to our employees internally (such as on the intranet) or externally in the press, newsletters, notice boards or promotional materials (consent will be obtained where appropriate)

If you agree to be the focus of a case study, take part in a training video, or agree for your photo to be used in publications or promotional materials, and this is not a requirement of your specific role, you will be asked for your consent and are able to withdraw your consent at any time if you change your mind.

Where Clarion need to publish your personal data as result of your role, for example on a notice board in a scheme so that customers know how to identify and/or contact you, we will tell you about this (and take any concerns into account) but will not ask for your consent as this is in relation to a contractual requirement.

- Complying with relevant legislation (e.g. The Health & Safety at Work Act) and equality of opportunity and diversity monitoring.

There is a legal obligation for us to process the information or to demonstrate to our regulator that we are fulfilling our obligations, for example around anti-discrimination laws.

- Management and administrative purposes:
  - Data will be processed for IT management including disaster recovery and business continuity procedures as well as system testing, for example, in the development of new IT systems or upgrades to existing ones. Where this is necessary, data will be anonymised in as far as possible and strict security controls will be put in place
  - Research - for example measuring staff satisfaction at work and planning and managing our operations

It is in our legitimate interests to understand how we are performing and to ensure we have a robust IT system in place so we can meet our mission statement and objectives.

- Communicating with you about your employment, including contacting you using

your personal contact details (including email, phone and text) where necessary, such as in situations where system issues will prevent you from logging onto Clarion systems.

It is in our legitimate interests to communicate with you and keep you up to date with news and events in order to meet our objectives around being an employer of choice.

We will also process confidential data about you including bank account information and criminal convictions where this is directly related to your employment.

We would like to highlight the following situations where personal information will be collected, accessed or processed:

1. Call recordings – where required for business purposes we operate call recording systems which record both incoming and outgoing calls, and depending on the functionality of the system in use, will record the screen itself. These are used for training and quality monitoring. Appropriate security controls are in place to safeguard the call recording systems in place, and all staff should be aware that any personal information disclosed during a telephone conversation could be captured on these systems. Where screen recording takes place, staff should minimise any screens they do not wish to be recorded.
2. Email – There will be occasions where access to your email account (or to results of email searches) will be granted to your line manager or other authorised member of staff) for example during periods of staff sickness, investigations into staff conduct or to facilitate response to a Subject Access Request. Requests for access to staff email accounts require appropriate approval before this can be granted, in line with relevant policies.
3. Tracking Communications - To help us improve our Internal Communications to colleagues, our Communications Team are able to view open and click rates on our email communications. We are able to use this data to see how different areas of the business engage with our communications and identify changes we might be able to make to improve engagement. On the whole, this data is viewed at a high level, however, this will be provided at a more granular level with appropriate sign off. We do not track emails between individual staff, for example between you and your line manager or between you and other colleagues.
4. Investigations into conduct – With approval from HR and/or Governance and Compliance, the following data will be provided as required; CCTV footage, emails and any available tracking data, instant messages, phone and internet usage, door entry records, content of network drives, vehicle tracking records, any other data, searches, or checks as deemed appropriate.
5. If you are eligible to select benefit(s) through CHG's flexible reward scheme, information you submit in support of your selection (e.g. sensitive health information in relation to a health cash plan) will not generally be accessible to CHG. Further details are outlined on the self-serve option available to you for managing your benefit selection(s). CHG will collect statistical information

about employees benefit selections to ensure we can manage our offering in accordance with any trends and preferences.

### Automated Decision Making and Profiling

There are some occasions where our computer systems are set up to use pre-programmed criteria to make automated decisions about you, for example determining your eligibility for a benefit. Where there is no human intervention, (no staff involvement in the decision process) and this has a legal or significant effect on you, you have a right to challenge the validity of any decisions made in this way and / or to ask us not to process your information in this way. Please contact us for more detailed information or to find out if you meet the criteria to opt out.

### **3. Special Categories of Personal Data**

Clarion sometimes processes special category personal data about you. Special categories of personal data are: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation. We also treat information about criminal convictions or offences including cautions as special category data.

Where Clarion processes this type of data about you it will do so either:

- Where we are permitted or required to do so by law – please see below
- With your consent
- Where we need to protect the vital interests (i.e. the health and safety) of you or another person
- Where you have already made your personal information public
- Where we or another person needs to bring or defend legal claims and/or
- Substantial public interest grounds

To process personal data about criminal convictions or offences, we must have both a lawful basis for the processing and either legal authority or official authority for the processing.

We use this data to ensure employment services are delivered appropriately and to monitor equity, diversity and inclusion. In the case of certain health information, this will be needed for health and safety purposes.

We will apply additional security and confidentiality measures when processing your special category data.

As an employer, Clarion is permitted to process your special category data where the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law. Clarion is also permitted by law to process this data for the assessment of the working capacity of the employee for example where we need to provide background data to Occupational Health who will be carrying out an assessment.

Where provision of this information is optional, we will make this clear at the point of collection and we will ask for your specific informed consent at the time of collecting this type of data.

Where you provide consent for us to process special categories of data, you have the right to withdraw this consent at any time.

There will be times where we will not need your consent to process (including sharing) this type of data. This will apply where we are permitted or required to do so by law, for example under Health and Safety Legislation or where processing of this data is necessary in order for us to carry out our obligations under employment law, for example to offer reasonable adjustments.

#### **4. How do we protect your information?**

We will apply appropriate technical and organisational measures to protect your personal information. For example, we have systems in place to ensure that access to personal information is restricted to authorised individuals on a strictly need-to-know basis.

When we need to share personal data with our third party suppliers, our relationships are governed by our contracts with them which include strict data sharing and confidentiality protocols.

#### **5. Sharing your personal information**

Sometimes we need to share personal information we hold about you with other organisations that we work with or who provide services on our behalf. When sharing information we will comply with all aspects of data protection law.

Where 'sharing' is in our legitimate interests:

- We will share your personal information with relevant teams and departments within CHG in order to manage your employment, for example Payroll.
- We will make your work related contact details (including job title, email address, phone numbers) available to staff within CHG on Outlook and on the Intranet.
- Where CHG have chosen to outsource a business function to a 3<sup>rd</sup> party provider, we will share relevant information with them. For example where we appoint a 3<sup>rd</sup> party to carry out a staff survey on our behalf or where a 3<sup>rd</sup> party IT supplier requires access to our systems to support, test or develop these systems.

Additionally, your personal information will be shared:

- Where we are *permitted* to do so by law, including sharing information with the police or agencies such as the National Fraud Initiative. More information can be found on the work undertaken by the Cabinet Office at: <https://www.gov.uk/government/collections/national-fraud-initiative> Where reasonable to do so, we will give prior notice of such exercises and provide links to further information.

- Where we are *required* to do so by law, for example, the provision of data to Government Departments such as HMRC and compliance with valid legal processes such as court orders. (Please also see Subject Access Request below)\*
- To meet our regulatory requirements.
- In response to emergency situations or where necessary to protect the vital interests of a person or group of people.
- Where the personal information is already publicly available.
- Where we have your consent to do so. (Please see below)\*\*

\* Subject Access Requests – Where reasonable, we may also release personal information in connection with Subject Access Requests made by service users or other staff members under data protection legislation. Information released may include information such as names, job titles, internal or external emails, file notes, reports, call recordings and CCTV footage.

\*\*Consent - Where appropriate, we will seek your explicit consent to share data – for example to share your Occupation Health report with your line manager. Where provided, consent can be withdrawn at any time by speaking with HR.

There are occasions where we need to process your information outside of the European Economic Area (EEA), for example where we use a third party computer system supported by employees in the USA. Where we do this we will take all necessary steps to ensure that your information remains secure. You can ask us for more information about how our International Processing arrangements affect you by using the contact details below.

## **6. How do we manage your personal information?**

We will treat your personal information fairly and lawfully in line with data protection legislation. Your data will be:

- Processed for limited purposes
- Kept up-to-date, accurate, relevant and not excessive
- Not kept longer than is necessary
- Kept secure

You should regularly check Workday to ensure that your personal information and emergency contacts are accurate and up to date and, where you are unable to make changes yourself, you must advise HR of any changes to your personal information during the course of your employment.

## **7. Contact Arrangements and promotion of our services**

We will routinely use your contact details to send you information and communicate with you about your employment including services and benefits available to you as an employee.

We will also use your personal contact details stored on Workday where we need to contact you for reasons relating to business continuity, such as where we need to advise you that service disruption will prevent you from logging onto Clarion systems.

Your personal information will not be passed to external organisations for marketing or sales purposes without your prior express consent.

## **8. How long will you keep my data?**

We only hold records while you are employed with us and for a set period afterwards. This allows us to meet our legal obligations and enables us to resolve any follow up issues.

Personal information about unsuccessful candidates will be held for 6 months after the recruitment exercise has been completed, it will then be destroyed or deleted. We retain anonymised statistical information about applicants to help inform our recruitment activities, but no individuals are identifiable from that data.

Please refer to the Document Retention Policy (based on National Housing Federation guidance, legal requirements and best practice) which is available on the Intranet for specific information about the length of time we keep different types of data. If you do not have access to the Intranet, you can ask us for further information about this.

## **9. Your rights in relation to your data**

Clarion is committed to upholding your rights in respect of your personal data.

### **The right to be informed**

Through the provision of this privacy notice, we will be open and transparent about how and why we use your personal information.

### **The right of access**

You have a right to ask us what personal information we hold about you and to request a copy of your information. This is known as a 'subject access request' (SAR).

The best way to do this is to put your request in writing or ask us for a copy of our template form. When a Subject Access request is made, we will take reasonable steps to verify your identity before we can proceed so you may wish to submit a copy of your photo ID with your request to save time.

If you are seeking to obtain specific information (e.g. about a particular matter or from a particular time period), it helps if you clarify the details of what you would like to receive in your written request. Very broad requests are likely to require clarification so we can make sure we know what information you require.

If someone is requesting information on your behalf they will need written confirmation from you to evidence your authority for us to release this and proof of ID (both yours and theirs).

Where you are unable to put your request in writing, you can contact HR to arrange for your request to be documented on your behalf.



If you choose to make a verbal SAR request, please contact HR who will record this for you and then send you a copy of the request to verify and attach ID (if necessary) before we start processing your request.

We generally have up to 1 calendar month within which to provide you with the information you've asked for (although we will try to provide this to you as promptly as possible). In response to SARs, we will provide you with a copy of the information we hold that relates to you. Please note, information sent and received by you in the normal course of your role will not generally constitute your personal data and will therefore not be provided to you. Please ask us if you have any questions about this or provide us with explanation along with your request as to why this data may be personal to you given the context.

It's important to note, that not all personal information will be released as there are 'exemptions' within the legislation which allow us to refuse to comply with your subject access request in certain circumstances. If we are unable to comply with your request then we will explain this to you. For example if information has been destroyed in accordance with our data retention policy or if information is legally privileged (such as confidential discussions between Clarion and its legal advisors in the course of seeking advice). Data will also be redacted or summarised where necessary, for example, to remove any reference to other third parties.

### **The right to rectification**

You can ask us to rectify your personal data if it is inaccurate or incomplete. Please help us to keep our records accurate by keeping us informed if your details change.

### **The right to erasure**

The right to erasure is also known as 'the right to be forgotten'. In some circumstances, you can ask us to delete or remove personal data where there is no compelling reason for its continued processing. This is not an absolute right, and we will need to consider the circumstances of any such request and balance this against our need to continue processing the data. Our response will also be guided by the provisions of our retention schedule.

### **The right to restrict processing**

In some circumstances you can ask us to restrict processing, for example

- if you disagree with the accuracy of personal data
- if we're processing your data on the grounds of legitimate interests (as detailed earlier), and whilst we consider whether our legitimate grounds override those of yours.

### **The right to data portability**

In some situations, you can ask us to move, copy or transfer personal data we hold about you to another organisation. Please contact us to discuss.

### **The right to object**

You can tell us if you object to our processing of your personal data:

- based on legitimate interests
- for the purpose of direct marketing (including profiling);

### **Rights in relation to automated decision making and profiling.**

Where a decision which has legal or significant effect on you is made solely by way of

automated means (i.e. there is no human intervention in a computer's decision) you have the right to object to this and depending on the reason for processing, either ask that we stop doing this or we show that we have implemented suitable measures to protect you, for example by explaining how the decision has been made and checking that the system is set up and functioning correctly.

## **10. Further information**

For further details on your rights, or if you have any questions or concerns about how and why we process your data, you can contact us using the details below.

Data Protection Team  
Clarion Housing Group Ltd  
6 More London Place, Tooley Street  
London  
SE1 2DA

[dataprotection@clarionhg.com](mailto:dataprotection@clarionhg.com)

Alternatively, if you want to raise a complaint about our processing of your data or would like to seek an independent view, you can contact the Information Commissioner:

Wycliffe House  
Water Lane  
Wilmslow, Cheshire  
SK9 5AF  
Phone: 0303 123 1113  
Email: [casework@ico.org.uk](mailto:casework@ico.org.uk)  
Website: [www.ico.org.uk](http://www.ico.org.uk)