

Candidate Privacy Notice



What is the purpose of this document?

Estuary Housing Association is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will be retained. It provides you with certain information that must be provided under the General Data Protection Regulation ((EU) 2016/679) (GDPR).

Data protection principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided on our application form (if you have applied for employment directly), including name, title, address, telephone number, personal email address, employment history, qualifications, and reference details.
- The information you have provided to us in your curriculum vitae and covering letter (if you have applied for employment via a recruitment agency)
- Any information you provide to us during an interview and / or assessment process

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, age group, marital status, disability, sexual orientation, gender and caring responsibilities.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, the candidate.
- Your recruitment agency (if applicable), from which we collect the following categories of data: CV and associated application documentation;
- GBG plc (umbrella body for Disclosure & Barring Service [DBS] checks) in respect of personal data and criminal convictions (if the role requires a DBS check);
- Disclosure and Barring Service in respect of criminal convictions (if the role requires a DBS check);
- Team Prevent (occupational health provider) in respect of medical and health records; this only applies after you have been offered a post;
- Your named referees, from whom we collect the following categories of data: Dates of employment, job title, salary, description of duties, attendance and performance;
- The recruitment software we use via this website is supplied by Net-Worx (2001) Ltd (trading as network) and they are defined as a Data Processor under GDPR. They will only process your data in accordance with our instructions
- Networkx can be contacted at: The Engine House, Wharfebank Business Centre, Ilkley Road, Otley LS21 3JP
- The Data Protection Officer for networkx is Rob Baker and can be contacted at dpo@networkxrecruitment.com

How we will use information about you

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

It is in our legitimate interests to decide whether to appoint you to role since it would be beneficial to our business to appoint someone to that role. We also need to process your personal information to decide whether to enter into a contract of employment with you.

Having received your application form (or CV if you have applied through a recruitment agency) we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role.

If we decide to offer you the role we will then take up references, carry out a Disclosure & Barring Service check (if applicable), obtain a minimum of 2 professional references, verify your professional qualifications (if applicable), verify your right to work in the UK and obtain fitness for work clearance from our occupational health provider before confirming your appointment.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a DBS check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

How we use particularly sensitive personal information

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Information about criminal convictions

If you are applying for a role which requires an enhanced DBS check, we envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history if we would like to offer you the role (conditional on checks and any other conditions, such as references, being satisfactory). We are required to carry out a criminal record check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. The basis for doing so is as follows:

- We are legally required under the Protection of Vulnerable Groups Act 2006 and Health & Social Care Act 2014 to carry out enhanced criminal record checks for those carrying out work which is deemed to be regulated activity.
- The role is one which is [listed on the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (SI 1975/1023)] [and is also specified in the Police Act 1997 (Criminal Records) Regulations (SI 2002/233)] so is eligible for an enhanced] check from the Disclosure and Barring Service.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data sharing

Why might you share my personal information with third parties?

Personal details you provide in this registration:

- Will be made available to us and our processors
- Will by preference be searchable on our candidate database
- Will allow you to optionally receive notifications on relevant jobs you are seeking
- Will be used for communication with you regarding recruitment
- Will be used for statistical analysis

You have the right to remove your details from our candidate database at any time by contacting the Human Resources department on 0300 3045000 or via email to peopleandchange@estuary.co.uk.

Although we may provide your information to service providers that handle information on our behalf, we will not share the information with third parties for secondary or unrelated purposes unless otherwise disclosed at the point of collection and not without having gained acceptance at the point of collection.

We may share your personal information with online testing providers as part of the selection process.

We will also share information with the following third parties, which only apply after you have been offered a post with Estuary:

- An umbrella body for Disclosure & Barring Service [DBS] checks) in respect of personal data and criminal convictions (if the role requires a DBS check);
- The Disclosure and Barring Service in respect of criminal convictions (if the role requires a DBS check);
- An occupational health provider in respect of medical and health records, in order to confirm your medical fitness to undertake the role and any reasonable adjustments you may require in accordance with the Equality Act 2010.

All our third-party service providers in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Specific information on third-party providers can be supplied upon request.

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, altered, disclosed, used or accessed in an unauthorised way. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality. [Details of these measures may be obtained from the Human Resources department].

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will retain your personal information for a period of 12 months after we have communicated to you our decision about whether to appoint you to the role. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our Document Retention policy and applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your rights in connection with personal information

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

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Human Resources Department in writing.

Right to withdraw consent

When you applied for this role, you provided consent on the date you submitted your application to us processing your personal information for the purposes of the recruitment exercise. You have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact the Human Resources Department. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely.

Data protection officer

Estuary has appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO, email: dpo@estuary.co.uk You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.