

Abri's Job Applicant Privacy Notice

V.3 03/07/25

Next review date 24/11/26

Abri is committed to protecting your privacy and takes its responsibilities regarding the security of your information very seriously. This Privacy Notice sets out how we will use and protect all information relevant to you, which we collect from you during the course of your application to work for us.

Throughout the rest of this Notice we will refer to you as the 'Applicant'.

We process Applicant information in accordance with relevant data protection and privacy laws (notably the UK General Data Protection Regulation, or 'GDPR', the Data Protection Act 2018 and the Data (Use and Access) Act 2025 - all of which together we refer to as data protection law).

Who we are

When we say Abri, 'we' or 'us' in this policy, we're generally referring to Abri Group and all the housing providers that make up Abri including Abri Group Limited, The Swaythling Housing Society Ltd, Octavia Housing and the Octavia Foundation (collectively 'Abri').

Under GDPR Abri are the Data Controllers of the personal information we hold about job applicants, and where an applicant has applied for a position using the Networx website, Iris Software Group Ltd (trading as 'Networx') is the data processor. Networx will only process your data under our instructions.

The data we collect

Abri recruits in conjunction with our preferred recruitment partner, Networx. When utilising the Networx website and submitting applicant information, you are agreeing to the use of such data in accordance with this privacy notice.

As defined by the GDPR, Abri is the Data Controller and ultimately responsible for ensuring the data you provide is kept secure, processed correctly and that you understand your legal rights in relation to that data. As part of our Data Controller responsibilities we have an assigned Data Protection Officer.

Abri's Data Protection Officer can be contacted at abridataprotection@abri.co.uk

The Data Protection Officer for Networx can be contacted at dataprotection@iris.co.uk

Abri will collect from you the following personally identifiable data that is specifically and voluntarily provided by you to us to support your job application, including (but not limited to):

- **Personal Details** - including name, address, D.O.B, marital status and gender;
- **Contact Details** - including personal email addresses and personal telephone numbers;
- **Previous employment details** - including your CV/application form providing details of previous workplaces, roles and employment history;
- **Experience and qualification details** - including your qualifications, skills, experience, professional body memberships and accreditations;
- **Job-related details** - including responses to behavioural or technical related questions; and
- **Eligibility to work details** - including proof that you are eligible to work in the UK, which could include passport or other documentation.

In collecting this information, we rely on the legal basis of the legitimate interests of Abri in carrying out an informed and fair recruitment process for job vacancies.

We may sometimes collect additional information from third parties or externally hosted sources, including: former employers or any referees you direct us to; the Disclosure and Barring Service; door entry systems; swipe card systems; CCTV; access control systems; remote access systems; and video conferencing and communication or collaboration platforms that may be used in the interviewing process.

Some of the information which we will collect may be examples of special categories of personal data (also referred to as 'sensitive personal data'). This may include:

- Information about your **race, ethnicity, religious belief and sexual orientation** which we monitor for purposes of ensuring equality, diversity and inclusion;
- **Criminal records history** - including, where applicable to the role you are applying for, whether you have any:
 - unspent criminal convictions, reprimands or cautions, together with any information held by the police which the Chief Officer deems relevant to the role (including where relevant if the applicant is barred from working with children or vulnerable adults) if the role requires an enhanced DBS check;
 - unspent convictions, cautions reprimands and final warnings if the role requires a standard check; or
 - unspent convictions and conditional cautions if the role requires a basic check.

- **Health details** - including whether or not you consider yourself to have a disability or impairment for which the organisation needs to make reasonable adjustments during the recruitment process.

We will only use your sensitive personal data in the following ways and based on the specified lawful bases:

- We will use information about your race or national or ethnic origin, religious beliefs and sexual orientation to ensure meaningful diversity and inclusion monitoring and reporting, in accordance with our public sector equality duty under the Equality Act 2010, and in accordance with substantial public interest.
- We will consider whether we need to provide appropriate disability adjustments during the recruitment process, to comply with our legal obligations as an employer and where it is needed in the public interest (such as equal opportunities monitoring) and
- We will use information about any unspent criminal convictions to determine your suitability for certain roles, bearing in mind our duty to safeguard vulnerable customers and to ensure high levels of proven trustworthiness for roles of a fiduciary nature, in accordance with substantial public interest.

Where we collect this data from

Abri collects this data during the recruitment process in a number of ways, for example:

- from documents or information supplied by the applicant before during and after interviews, notably in the form of CVs, answers given to questions raised in assessments, copies of identity documents and proof of right to work documents
- from information supplied by third parties (with the applicants prior knowledge and consent) who have direct experience of the applicant via personal or professional relationships and contact, notably in the form of references ; or who hold information about the applicant which is relevant to the recruitment, notably the Disclosure and Barring Service
- from open source information, - notably the internet - when verifying an applicant's professional background and public achievements, and evaluating their digital footprint in those cases where it is deemed preferable to identify any behaviours that may be inconsistent with the standards of professional behaviour required for the position they have applied for, or which may pose a risk to Abri's reputation.

References

Abri will only seek references once a job offer has been made and once the applicant has provided contact details for the proposed referees.

The provider of the reference remains the data controller of the information and/or opinions provided in the reference. For more information about the implications of this, see the section below entitled '**Your rights and how you can access the data we hold about you.**'

Where we will store this data

Your personal information will be stored on the Networx system, which ensures generally accepted standards of technological security for the purpose of protecting data provided by visitors to its website from misuse, loss or corruption. Only authorised Networx and Abri colleagues have access to personally identifiable data submitted through the website. Such colleagues are contractually required to maintain the confidentiality of this data.

How long will we hold your data

We will only retain your information for as long as is necessary to fulfil the purposes set out in this Privacy Notice.

Interview and assessment records for unsuccessful applicants will be retained for a maximum period of six months after the vacancy has closed.

Records for successful applicants will be transferred to their personal Abri HR file and another privacy notice will then apply to their data as an Abri colleague.

Your candidate account will be deactivated after 12 months of inactivity. At the same time as this, your data will be fully anonymised.

Back-Ups

All our data is backed up regularly as part of our measures to ensure compliance with your right to have your data kept secure and protected against any threat to its integrity. Data held in our back-ups may exceed the retention period set for the same data when it is part of our live systems. This is because our back-ups are kept for 7 years, no matter what the particular retention period applicable to individual records held within them. However, acting in accordance with ICO advice, we believe that these comply with our legal obligations towards our colleagues because:

- while held as back-up, this data is deemed ‘beyond use’; and
- if the back-up files are ever restored to live systems (eg. in the case of a cyber incident affecting the integrity of our live records) we will undertake sanitization of the restored data to delete from it any data which is either beyond its retention period, or should be deleted because it formed part of a job applicant record that was erased under the data subject’s right of erasure (see below).

Why we need this data

Abri needs to process the types of data listed above for a variety of purposes for which we have a ‘lawful basis’. This data enables Abri to:

- assess your skills, qualification and suitability to the role you have applied for;
- communicate with you during the recruitment process;
- keep records of our hiring processes;

- carry out our obligations and exercise specific rights in relation to employment including carrying out statistical analysis; and
- comply with our legal obligations such as to prevent fraud.

Abri will always comply with data protection laws. We will ensure the data we hold about you will be:

- used lawfully, fairly and transparently;
- collected only for, and will be relevant to the purposes explained to you;
- accurate and kept up to date;
- kept only for as long as required; and
- kept securely.

Technology Informed Decision Making

We may use some automated screening tools (including AI) as part of the application process. The answers you provide to one or more questions (excluding any related to special categories or any equal opportunities issues) may result in your application being scored less favourably or in some instances automatically declined. In particular we may ask you to either exclude or limit the use of AI in generating content to support your application. We use technology that will enable us to determine if you followed these instructions, and - where some use of AI was allowed - to determine the extent to which you did use it. This technology is used to help us manage a high volume of applications we receive for some roles and to ensure that applicant capabilities are being fairly measured and compared in the selection process. When requested, we will discuss with applicants the scoring or selection decisions that have been informed by the use of this technology in order to ensure that outcomes are as fair as possible bearing in mind all factors which the applicant feels should be taken into account. The reason for any application being declined on this basis will be made clear in your candidate account, and you are entitled to ask for it to be reviewed personally by a member of our recruiting team.

Who we share your data with & why

Your data will be accessed internally by a tightly limited number of Abri colleagues involved in undertaking a fair and legally compliant recruitment process. This includes making it accessible to Abri HR, Abri directors and managers involved in the recruitment process, and any other colleagues where access to the data is necessary for the performance of their roles.

Abri will not share your data with third parties unless your application is successful and results in an offer of employment. The organisation may then share your data with former or current employers you have nominated to provide references. However if you do not nominate referees from your current or recent employers which are satisfactory to Abri we may in some circumstances have to withdraw the offer of employment. We verify data with the Disclosure and Barring Service to obtain necessary criminal records checks where

appropriate for the role. We also share data with third party occupational health advisors to ensure we meet our health and safety responsibilities, and with third parties that conduct Right to Work checks, and where appropriate driving licence and motor insurance checks.

Networkx and Abri will not share your data with third parties for secondary or unrelated purposes unless otherwise notified clearly at the point of collection and not without having gained your consent to this at the point of collection.

How will we secure your data?

Abri takes the security of your data seriously. It has policies and procedures in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our colleagues in the proper performance of their duties.

Networkx have in place reasonable commercial standards of technology and operational security along with internal policies and procedures to protect all data provided by visitors to its website and applicants from loss, misuse, alteration or destruction.

Your rights and how you can access the data we hold about you

Abri and Networkx are dedicated to providing reasonable access to applicants who wish to review the personal data collected and retained when they apply via the Networkx website, and to correct any inaccuracies it may contain. Applicants who choose to register may access their profile, correct and update their details, or delete their details at any time by accessing their personal profile and using their secure login. In all cases, even after the recruitment for a position has completed, Abri will treat applicants' requests to access or change data in accordance with applicable legal requirements and will meet the deadline for doing so - 30 days from the date of the request, unless an extension may be justifiable under data protection law.

You have the following rights in relation to the way your personal data is handled:

- the right of erasure, or to be forgotten (but please note the explanation re back-ups);
- the right to rectification if data is inaccurate or out of date;
- the right of data portability (to obtain and reuse your personal data);
- the right to object, in certain cases, to Abri's handling of your personal data;
- the right to withdraw your consent with regards to the handling of your personal data, where we have relied on consent as the lawful basis for processing that personal data;
- the right to ask for a copy of the data we hold about you (Subject Access Request); and
- the right to lodge a complaint with a supervisory authority - the ICO - if you believe that we have not processed your personal data in accordance with our obligations under data protections laws.

Where you exercise your right to object or withdraw your consent we may continue to process your personal data nonetheless where we are permitted or required by law or regulatory requirements to do so. In such a case, we will not process more personal data than is required under the circumstances.

Similarly the rights of erasure and rectification are subject to certain qualifications and conditions, which - if met - may mean that we do not erase or rectify in precisely the way you have requested that we do so. If you wish to know more about this please ask us to share with you copies of our Data Erasure and Data Rectification Procedures, both of which have been written to comply with applicable data protection laws.

Your right to access personal data we hold about you may be subject to certain limitations and exclusions, notably:

- When we are not the data controller for information that has been supplied to us as part of the recruitment process, eg. for references supplied in confidence by former employers, we will not be able to disclose the reference to you, however you may still request disclosure from the organisation or individual who provided it to us.
- We will redact to remove from disclosure the personal details of third parties whose details form part of your information record, unless they have consented to us releasing them to you.
- We will redact to remove any information included in your recruitment record that is covered by legal professional privilege, or forms part of a record that is otherwise exempted from disclosure under data protection laws.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to Networx or Abri during the recruitment process. However, if you do not provide the information requested during the process, it may not be possible for us to process your application properly or at all.

Changes to our Privacy Notice

We reserve the right to modify or amend this privacy notice at any time and for any reason, providing it maintains compliance with the UK General Data Protection Regulation 2020, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

If you would like to exercise any of your rights, you can contact our Data Protection Officer at abridataprotection@abri.co.uk

If you remain dissatisfied, you have the right to refer the matter to the Information Commissioner (www.ico.org.uk).

By ticking the box and continuing with your application, you are confirming that you have read the terms in this privacy notice.