ABBEYCROFT

RECRUITMENT PRIVACY NOTICE

This Privacy Notice sets out what personal information is processed by Abbeycroft and for which purposes during the recruitment process. It also explains the rights you have and how to exercise them.

Abbeycroft collects and processes personal information relating to job applicants. This information is considered "personal data" under the UK General Data Protection Regulation (UK GDPR).

Abbeycroft is committed to being transparent about how it collects and uses personal data and to meeting its data-protection obligations.

Our Safer Recruitment Policy, which is available on our website or by emailing human.resources@acleisure.com, should be read in conjunction with this Privacy Notice.

Data controller (responsible for determining what and how personal information is processed)

Abbeycroft
Lordscroft Lane
Haverhill
Suffolk
CB9 0ER

Data Protection Officer:
Claire Turnbull
Email: information.officer@acleisure.com

What information does Abbeycroft collect?

Abbeycroft collects and processes a range of personal information about you as part of the recruitment process, including:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current remuneration and benefit entitlements, where relevant;
- information about whether you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;

- information about your nationality and entitlement to work in the UK; and
- equal opportunities monitoring information, including information about ethnic origin, sexual orientation, health or religion or belief.

Some of this information is classed as special category personal data and is subject to additional legal protections.

How personal information is collected

Abbeycroft collects personal information in a variety of ways. For example, information may be collected through application forms and CVs, from identity documents such as passports or driving licences, services used to prove your identity or right to work in the UK, or through interviews, assessments and online tests.

The organisation may also collect personal data from third parties, such as references supplied by previous employers and, where legally required, information obtained through criminal records checks.

Information from third parties is normally sought only after a conditional offer of employment has been made.

Personal data is stored securely on recruitment files, HR management systems and other authorised IT systems.

Why does Abbeycroft process personal data?

Abbeycroft processes personal data for the purpose of managing its recruitment processes and deciding whether to appoint candidates.

Personal data is processed on the following lawful bases:

To take steps prior to entering into a contract

Personal data is processed to take steps before entering into a contract, including assessing your suitability for a role and communicating with you about the recruitment process.

To enter into a contract

Where an offer of employment is made, personal data is processed to enable Abbeycroft to enter into a contract with you.

To comply with legal obligations

Your data is processed to meet legal obligations, including checking your eligibility to work in the UK, your criminal records history (where relevant), and complying with responsibilities under employment and equality legislation.

Based on legitimate interests

Abbeycroft has a legitimate interest in processing personal data during recruitment to:

- manage recruitment activities efficiently;
- assess candidates against role requirements;
- keep records of recruitment decisions;
- respond to and defend against legal claims.

Where personal data is processed on the basis of legitimate interests, the organisation has considered whether those interests are overridden by your rights and freedoms and concluded that they are not.

Special category data

Health information is processed only where necessary to make reasonable adjustments for candidates with disabilities and to meet obligations under employment law.

Equal opportunities monitoring information is processed for the purposes of monitoring equality and diversity. Provision of this data is voluntary and it is anonymised or aggregated wherever possible.

For some roles, Abbeycroft is legally required to process information about criminal convictions and offences.

Abbeycroft will not use your personal data for purposes unrelated to the recruitment processes necessary for the post to which you have applied.

Who has access to data?

Your personal data will be shared internally for the purposes of the recruitment exercise. This includes HR staff, interviewers, managers in the business area with a vacancy, and IT staff where access is required to perform their duties.

Personal data will not normally be shared with third parties unless a conditional offer of employment is made. In those circumstances, data may be shared with previous employers to obtain references, with our onboarding service providers, and with the Disclosure and Barring Service where criminal records checks are required.

Some recruitment systems used by Abbeycroft may involve processing personal data outside the UK, including in the United States. Where personal data is transferred internationally, it is protected using approved safeguards, and lawful transfer mechanisms.

How does the organisation protect data?

Abbeycroft takes the security of your data seriously. Appropriate technical and organisational measures are in place to try to protect personal data from loss, misuse, unauthorised access or disclosure. Access to HR and payroll systems is strictly controlled and can only be accessed by named individuals. Where we engage third parties to process data on our behalf, they do so on the basis of written instructions, under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

If your application is unsuccessful, Abbeycroft will retain your personal data for up to six months after the conclusion of the relevant recruitment process. This allows the organisation to respond to queries or legal challenges. At the end of this period, your data will be securely deleted or destroyed.

If your application is successful, personal data collected during recruitment will be transferred to your personnel file and retained in accordance with the Employee Privacy Notice.

YOUR RIGHTS

As a data subject, you have the right to:

- access your personal data and obtain a copy;
- request correction of inaccurate or incomplete data;
- request erasure of your data, where legally permitted;
- object to processing where the organisation relies on legitimate interests;
- request restriction of processing in certain circumstances; and
- request data portability where processing is based on pre-contractual steps.

You can exercise these rights by emailing information.officer@acleisure.com.

If you believe Abbeycroft has not complied with data-protection law, you have the right to complain to the Information Commissioner's Office (ICO):
www.ico.org.uk | Tel: 0303 123 1113

What if you do not provide personal information?

You are under no statutory or contractual obligation to provide personal data during the recruitment process. However, if you do not provide the information requested, Abbeycroft may not be able to process your application or consider you for employment.

Automated decision-making

Recruitment decisions are not based solely on automated decision-making without human involvement.

This Recruitment Privacy Notice will be reviewed regularly and updated where necessary to reflect legal, regulatory or organisational changes.

Last updated May 2026