Privacy Notice for Job Applicants

Version Control

Version	Date	Comments	Author
1.0	01 July 2023	Approval	HR
1.1	18 January 2024	Updated & Approved	HR
1.2	12 March 2024	Updated & Approved	HR
1.3	01 July 2024	Annual Review	HR
1.4	01 June 2025	Update DPO	HR

Oxbury Bank Plc is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority with Financial Services Register number 834822. Registered in England and Wales (Registered Number 11383418). Registered Office: One City Place, Queens Road, Chester, CH1 3BQ. VAT Registration Number GB 411 9831 06.

Oxbury

Job applicant Privacy Notice

Oxbury Bank Plc is aware of its obligations under the General Data Protection Regulation (GDPR) and current data protection legislation and is committed to processing your data securely and transparently. This privacy notice sets out, in line with data protection obligations, the types of data that we collect and hold on you as a job applicant. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

Data controller details
Oxbury Bank Plc is a data controller, meaning that we determine the purpose and processes to be used when processing your personal data. We are registered with the Information Commissioner's Office with reference ZA511261. Our contact details are as follows: Oxbury Bank Plc, One City Place, Queens Road, Chester, Cheshire, CH1 3BQ. You can also contact us at privacy@oxbury.com.

Data protection principles
In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

Types of data we process
We may hold many types of data about you, including:

- Your personal details including your name, address, date of birth, email address, phone numbers
- Your photograph
- Gender
- Marital status
- Preferred pronoun
- Whether or not you have a disability or medical condition
- Information included on your CV including references, education history and employment history
- Documentation relating to your right to work in the UK
- Driving licence
- Bank details
- Ethnic origin
- Nationality
- Your Next of Kin contact information

How we collect your data
We collect data about you in a variety of ways including the information you would normally include in a CV or a job application cover letter, or notes made by our recruiting managers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies
Personal data is kept in personnel files and within the Company's HR system.

Special categories of data
In order for us to support you or as part of a legal obligation it may be required that special categories of data are processed, which is data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership and
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time, and you can do this by contacting the HR Team on HR@oxbury.com. There will be no consequences where consent is withdrawn.

Criminal conviction data
We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment should you be successful in obtaining employment.

We conduct Disclosure and Barring Service checks (DBS checks) for all roles to comply with our regulatory obligations to ensure prospective employees are suitable for the role in which they are applying.

Fraud checks – completed for all roles.
Personal information collected will be shared with Cifas who will use it to prevent fraud, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct. If any of these are detected, you could be refused certain services or employment. Your personal information will also be used to verify your identity. Further details of how your information will be used by Cifas, and your data protection rights, can be found at www.cifas.org.uk/fpn or by requesting a copy of the Fair Processing Notice. Oxbury shall notify the individual of any matter revealed on a credit or fraud check which may lead to withdrawal of a conditional offer of employment or termination of

employment. Oxbury will direct the individual to the credit reference agency or Cifas should the individual wish to make a data subject access request to obtain the information held about them by the agency.

Credit checks – only conducted for certain roles
Credit checks may be completed prior to employment and as deemed appropriate by Oxbury thereafter, using credit reference agencies such as Experian. Oxbury undertakes to notify the individual of any matter revealed on a credit check which may lead to withdrawal of a conditional offer of employment or termination of employment. Oxbury will direct the individual to the credit reference agency should the individual wish to make a data subject access request to obtain the information held about them by the agency.

Periodic Screening
Employees may be periodically subject to background screening during their employment. Generally, such periodic screening will be limited to identity confirmation, credit checks, fraud checks and criminal background checks. The majority of periodic screening will be to support Oxbury meet its obligations under the Senior Managers and Certification Regime. CIFAS screening of all employees will be conducted at least annually.

If you do not provide your data to us
One of the reasons for processing your data is to allow us to carry out an effective recruitment process. Whilst you are under no obligation to provide us with your data, we may not be able to process, or continue with (as appropriate), your application.

Why we process your data
The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- to protect your interests and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data.

We need to collect your data to ensure we are complying with legal requirements such as:

- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- making decisions about who to offer employment to
- making decisions about salary and other benefits
- assessing training needs
- dealing with legal claims made against us

If you are unsuccessful in obtaining employment, your data will not be used for any reason other than in the ways explained in relation to the specific application you have made.

Sharing your data
Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties with regard to recruitment. This includes, for example, the HR department, those in the department where the vacancy is, who is responsible for screening your application and

interviewing you, the IT department where you require access to our systems to undertake any assessments requiring IT equipment.

In some cases, we will collect data about you from third parties, such as employment agencies. Your data will be shared with third parties if you are successful in your job application. In these circumstances, we will share your data in order to obtain references as part of the recruitment process and obtain credit, fraud and criminal records checks.

Due to the global nature of our HR system, personal data may be shared with bodies outside of the European Economic Area. These countries are US and India. The company take steps and implement measures to keep your personal information secure by

- using safeguards such as the standard contractual clauses and ensuring processors are not permitted to extract or download or save data locally.
- protecting your rights and freedoms such as anonymising or pseudonymising personal data and withholding encryption keys.

Protecting your data
We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with data protection requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for
In line with data protection principles, we only keep your data for as long as we need it and this will depend on whether or not you are successful in obtaining employment with us.

If your application is not successful and we have not sought consent or you have not provided consent upon our request to keep your data for the purpose of future suitable job vacancies, we will keep your data for 12 months once the recruitment exercise ends.

If we have sought your consent to keep your data on file for future job vacancies, and you have provided consent, we will keep your data for 24 months once the recruitment exercise ends. At the end of this period, we will delete or destroy your data, unless you have already withdrawn your consent to our processing of your data in which case it will be deleted or destroyed, in line with our internal policies, upon your withdrawal of consent.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We have a separate privacy notice for employees, which will be provided to you and explains how we process your data as a successful employee.

Automated decision making
No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data
The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request, and send this to privacy@oxbury.com

- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the processing of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact privacy@oxbury.com.

Making a complaint
The supervisory authority in the UK for data protection matters is the Information Commissioner's Office (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire
SK9 5AF

Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

Data Protection Officer
The Company's Data Protection Officer is Robin Hill. He can be contacted on privacy@oxbury.com.