# Oxbury Employee Privacy Notice

The Company needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for Company management and administrative purposes only. We will store and use your information to enable us to run the business and to manage our relationship with you effectively, lawfully and appropriately during the recruitment process, whilst you are working for Oxbury and after your employment with the Company ends. This includes using information to enable us to comply with the employment contract, to comply with legal requirements, to pursue the legitimate interests of the Company and to protect our legal position in the event of legal proceedings.

Most of the information we hold will have been provided by you, but some may have come from other internal sources, such as managers, or from external sources, such as referees.

**What information do we hold and what is it used for?**
The sort of information we hold includes your CV or application form; references; passport or other documents to confirm eligibility to work in the UK; contract of employment and amendments to it; correspondence with or about you; information needed for payroll, benefits or expenses purposes; contact and emergency contact details; records of holiday, sickness or other absences; working hours from timesheets; information for equal opportunities monitoring; and records relating to your career history such as training records, qualifications, appraisals, disciplinary and grievance records.

Where necessary we may keep information relating to your health, which could include the reasons for absence and GP / hospital reports. This information will only be used to comply with health and safety and occupational health obligations. Eg to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also use this information to administer company sick pay.

During the course of carrying out your normal day to day duties, you will of course be referred to in many company documents and messages that are produced by and shared with you, your colleagues and third parties as part of normal Company business.

The Company does process data about special categories of personal information relating to racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union memberships, and sexual orientation. This information is collected anonymously so individuals cannot be identified. It is only used for monitoring the Company's performance against equality and diversity standards. Equality and diversity statistics drawn from this data may be provided to third parties as part of our response when tendering for jobs or applying for standards such as the RICS Chartermark.

**How is your information stored and who has access?**
Employee's personal information is stored in both electronic and paper form.

Paper documents are stored in a locked filing cabinet or cupboard in the office in Norwich. Electronic documents are stored using Sage software (Accounts, Payroll and HR) on a secure section of the Company server, and are protected by individual log-ons and passwords.

Only the HR & Practice Manager and Directors have access to the paper files and to the electronic records. In order to meet the Company's contractual and legal obligations in relation to pay, benefits and taxation, the Bookkeeper has access to employee financial information, but not other personnel records.

Documents or information about you may be shared with other people internally where this is necessary for the administration and management of the Company. Access will be via the HR Manager or a Director and only the information that is directly relevant will be shared.

Once you leave the company your personal information may be moved to a secure archive facility.

**Who do we share your information with?**
We will only share your personal data with 3rd parties if we are legally obliged to do so or where necessary to comply with our contractual obligations. For example, we share employee data with the Company Accountants (Sexty & Co) who process our payroll; and with the Pension Scheme Administrators (Smith & Pinching). We may also need to share data with our Insurance Brokers or Underwriters where that information is pertinent to our insurance provision. When we send information outside the Company it is emailed in password protected files and is only sent to named contacts.

**How long do we keep your personal information?**
Most employee data will be kept for 6 years after your employment has ended. It will be stored on site for 12 months and then moved to off-site archive storage. After 6 years all personal data will be destroyed except for basic information, such as job title and dates of employment, that may be required if the Company is asked to provide a reference to a future employer.

**What are your rights?**
You have the right to access the information we hold about you; to have any inaccuracies rectified; and to erase information which is incorrect or should no longer be held. You also have the right to object to and restrict processing of your data. However, be aware that if you do not provide information or allow us to process your data we may be unable to fulfil our legal and contractual obligations. If that is the case we will tell you about the implications of your decision.

If you want to access your personal information you can submit a Subject Access Request in writing to the HR & Practice Manager. The Company will either provide the

information requested, or will explain why there is a delay, within one month.

You have the right to lodge a complaint with the information Commissioners' Office if you believe we have not complied with the requirements of the General Data Protection Regulations with regards to your personal data.

**Who is the responsible for Data Protection?**
You are responsible for keeping your personal data up to date. You must inform the HR & Practice Manager of any changes to your personal data. For example, address, contact details, bank details etc.

Tim Boucher is the Board member with responsibility for Data Protection.