Data protection policy

As a Company we are committed to being transparent about how we collect and use data associated with our business, and to meeting our data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, consultants, volunteers, interns, apprentices and former employees and all other people who supply the Company with personal data, including customers, clients, suppliers and other business contacts.

All staff must read, understand and comply with this policy and any related policies, operating procedures or processes, privacy notices and attend any required training on its requirements. All staff operating at management level have a responsibility to set an appropriate standard of behaviour and to lead by example. They should ensure those they manage adhere to this policy and receive appropriate training to ensure such compliance.

As the Company processes 'personal data' of individuals, it is defined as a Data Controller for the purposes of the UK General Data Protection Regulation ("GDPR"). The GDPR places obligations on the way personal data is handled. As an employee of the Company you also have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if we have a valid condition of processing (e.g. consent obtained from the data subject, or a contract with them) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice). There are restrictions on activities with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

As a Data Controller the Company also remains responsible for the control of personal data collected even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations (including devices personally owned by members of staff). The Company has appointed Sonia Tyack, Personnel Manager, as the person with responsibility for data protection compliance within the Company. They can be contacted via the email address dataprotection@hrwallingford.com. Questions about this policy, or requests for further information, should be directed to them.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that data (or from that data and other information in our possession). It accordingly excludes anonymous data. Personal data can be factual or it can be an opinion.

"Processing" is any activity that involves use of personal data whether or not by automated means, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, genetic data and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The Company processes personal data in accordance with the following data protection principles:

- we process personal data lawfully, fairly and in a transparent manner.
- we collect personal data only for specified, explicit and legitimate purposes. We also process personal data for archiving, scientific, research or statistical purposes.
- we process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- we keep accurate and, where necessary, up-to-date personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- we keep personal data only for the period necessary for processing. We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company provides privacy notices to relevant individuals informing them about their rights, how it complies with its data protection obligations, how it collects and uses personal data, the reasons for processing personal data and the legal basis for any such processing. Such information may also be included in its contractual documents with third parties.

The Company must only use personal information for the purposes for which it was collected, unless it reasonably considers that it needs to use it for another reason and that reason is compatible with the original purpose. If the Company needs to use personal information for an unrelated purpose, it must notify the relevant individuals and explain the legal basis which allows it to do so.

The Company must maintain appropriate records of the processing activities for which it is responsible in accordance with the requirements of the General Data Protection Regulation (GDPR).

The Company will provide appropriate training to all staff about their data protection responsibilities. The level of training will reflect their role's access to personal data and responsibility for implementing this policy.

Conditions of processing and consent

We tell individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy policies. In order for the processing to be legal and appropriate we will ensure that at least one of the following conditions are met:

- the data subject has given his/her consent
- the processing is required due to a contract
- it is necessary due to a legal obligation
- it is necessary for the legitimate interests of the controller or third party and does not interfere with the rights and freedoms of the data subject

Where the Company processes "special categories" of personal data extra, more stringent conditions are met in accordance with Article 9 of the GDPR.

Personal data is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which we hold HR-related personal data are contained in our privacy notices.

Records of processing activities

The Company is required to maintain a record of processing activities which covers all the processing of personal data carried out ("data audit"). This contains details of why the data is being processed, the types of individuals about which information is held, who the information is shared with and when it is transferred to countries outside the EU.

Staff embarking on new activities involving the use of personal data that is not covered by one of the existing records of processing activities must add to the data audit and ensure compliance with this policy.

Individual rights

As data subjects, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request to allow them to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary.

If you make a subject access request, we will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you;
- to whom your data is or may be disclosed;
- for how long your personal data is stored;
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and
- whether or not we carry out automated decision-making and the logic involved in any such decision-making.

We will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise. If you would like additional copies, we may charge a reasonable fee.

To make a subject access request, you should send the request to dataprotection@hrwallingford.com. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within a period of one month from the date it is received. However, in some cases, such as where we process large amounts of your personal data, we may respond within three months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. An individual will not normally have to pay a fee to access their personal information or to exercise any of the other rights listed below. However, the Company may charge a reasonable fee if a subject access request is clearly unfounded or excessive due to the administrative cost of having to respond to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They have the right to:

- require the Company to correct inaccurate or incomplete personal data;
- require the Company to delete or stop processing their personal data where there is no good reason for the Company continuing to process it or where they have exercised their right to object to processing (see below);
- object to the processing of their personal data where the Company is relying on its legitimate interests (or those of a third party) as the legal ground for processing;
- request the restriction of processing of their personal data. This enables them to ask the Company to suspend the processing of their personal data, for example if they want the Company to establish its accuracy or the reason for processing it;
- object to specific types of processing if they can demonstrate grounds for objecting to the processing (For the processing of personal data for direct marketing, individuals have an absolute right to object.);
- not be subject to decisions based solely on automated processing (The Company does not presently use this method of decision making or profiling.); and
- request information about them is provided in a structured, commonly used and machine-readable form so that it can be sent to another data controller. This only applies to personal data that is processed by automated means (not personal records), to personal data which the data subject has provided to the Company and only when it is processed on the basis of consent or a contract.

To ask the Company to take any of these steps, the individual should send the request to dataprotection@hrwallingford.com.

If an individual believes that the Company has not complied with their data protection rights, they have the right to complain at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Data security

The Company takes the security of personal data seriously. The Company has appropriate technical and organisational measures and safeguards in place to prevent unauthorised or unlawful processing, to prevent personal data from being lost, accidentally destroyed, misused or disclosed, and to ensure that it is not accessed except by the Company's employees and other staff when necessary in the proper performance of their duties. We will regularly evaluate and test the effectiveness of these measures and safeguards. Data security should be undertaken in line with the IS Usage Policy and Security Policy.

You must comply with the Company's procedures and processes to ensure data security and also not act in a manner which may invalidate or render ineffective the Company's measures and safeguards.

Third parties

Where the Company engages third parties to process personal data on its behalf, the Company must ensure the third party provides adequate guarantees in terms of data security standards, policies, procedures, security measures in place, reliability and resources to implement appropriate technical and organisational measures to ensure personal data is processed in accordance with both companies' data protection obligations.

The Company must have in place a contract or other legal arrangement with the third party setting out the type of personal data that will be processed, the duration of the processing, the nature and purposes of the processing, the categories of data subjects, the obligations and rights of the Company, the specific tasks and responsibilities of the third party and the requirements around returning or deleting the personal data after completion of the contract.

International data transfers

Data Protection legislation restricts data transfers to countries outside the European Economic Area (EEA) and/or the UK in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

The Company may only transfer Personal Data outside the EEA/UK in very limited circumstances.

The Company operates globally and has offices and subsidiaries in locations such as the USA, China, Australia, Italy, India, UAE and Malaysia. The Company may from time to time transfer personal data from within the European Economic Area (EEA) and/or the UK to the Company's offices outside of the EEA/UK or to other people or companies.

To safeguard personal data the Company ensures that all offices, subsidiaries and affiliates enter into a group data protection agreement which will apply, where personal data is transferred to one of them. The Company will put provisions in place to make sure that when personal data is transferred it will be protected in the same way as it is protected before the transfer.

The Company aims to put in place a data processing agreement with any third parties which will also ensure similar protection for personal data.

Individual responsibilities

Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided to the Company changes, for example if an individual moves house or changes their bank details. The Company will update personal data promptly if an individual advises that their information has changed or is inaccurate. Where access is provided to the personnel system employees are expected to be responsible for ensuring that personal data that is held on the personnel system is kept up to date.

Individuals may have access to the personal data of other individuals and of our customers, suppliers, tenants, subcontractors and clients in the course of their employment, contract, volunteer period, consultancy agreement, agent agreement, internship or apprenticeship. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff and other individuals.

Staff who have access to personal data must:

- comply with the Company's commitments set out in this policy when processing personal data;
- promptly attend training sessions regarding data protection and data security as requested by the Company and ensure any team members for which you have management responsibility have attended appropriate training dependent on their role;
- process personal data on a need-to-know basis and for authorised and lawful purposes in accordance with the relevant privacy notices only;
- ensure that prior to transferring data to a third party or outside the European Economic Area there are adequate security measures in place in compliance with the relevant restrictions set out in this policy;
- ensure that when personal data is no longer needed for specified purposes it is deleted or anonymised in accordance with the Company's the data retention guidelines set out in the relevant privacy notice;
- comply with your obligations of confidentiality and the Company's information security measures, policies and procedures as put in place from time to time, including those relating to data security, password protection and encryption, use of and access to the Company's IT and communications systems, access to premises, use of personal devices for work purposes and use of removable storage devices;
- notify dataprotection@hrwallingford.com immediately in the event you become aware of or suspect there has been a personal data breach;
- notify dataprotection@hrwallingford.com immediately in the event you receive a request from an individual exercising their data subjects' rights detailed above. You must not disclose personal data requested without having first verified that person's identity;
- keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

- not store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee data, client data or other third party data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Data protection impact assessments and data protection by design

When considering a new processing activity or setting up new procedure or systems that involves personal data, GDPR imposes a "privacy by design" requirement, which the Company will comply with.

When appropriate, including where processing is likely to result in a high risk to an individual's rights and freedoms and in the event of all major system or business change programs involving the processing of personal data, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This may include the processing of large amounts of personal data, processing of special categories of personal data or monitoring publicly assessable areas (i.e. CCTV). The data protection impact assessment will include a description of the processing, its purposes, the Company's legitimate interests if appropriate, an assessment of the risks for individuals and the measures put in place to mitigate those risks. Where the impact assessment indicates the processing involves a high risk that cannot be mitigated by appropriate measures in terms of available technology and costs of implementation we shall consult the supervisory authority prior to the processing.

Data breaches

If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner without undue delay and, where feasible, within 72 hours of discovery. This will include any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the safeguards that the Company or a third party has put in place to protect it that poses a risk to the rights and freedoms of individuals. The Company will record all data breaches.

Every effort will be made to avoid personal data breaches however it is possible that mistakes will occur on occasions. Examples include:

- Loss of theft of data or equipment
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will tell affected individuals that there has been a breach without undue delay and provide them with information about its likely consequences and the mitigation measures the Company has taken.

Please note that it is crucial that you report any potential data breach as soon as you become aware of it, regardless of how serious you believe that breach to be. All individuals have an obligation to report actual or potential data breaches. To report a data breach please send an email to dataprotection@hrwallingford.com.

Data retention

The Company must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained. Individuals within the Company are responsible for ensuring appropriate retention periods for the information they hold and manage. Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance.

Training

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Contacts

In the first instance all enquiries or requests for further information or guidance relating to data protection should be directed to: dataprotection@hrwallingford.com.

Territory

This policy has been prepared principally with reference to the laws of England and Wales, but the Company is committed to compliance with the laws and regulations of all jurisdictions in which it operates. This policy shall accordingly be read and interpreted, as far as is possible, so that it is line with the applicable legal jurisdiction and the Company reserves the right to depart from the terms of this policy as may be necessary to comply with legal requirements.

Ridha Bentiba
Chief Executive Officer (Joint), HR Wallingford Ltd

Signed: 

Date: 10 July 2025

Review date: 10 July 2027