Data protection policy

Purpose

HR Wallingford is committed to being transparent about how it collects and uses data associated with its business, and to meeting its data protection obligations. This policy sets out HR Wallingford's 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 HR Wallingford with personal data

As HR Wallingford processes 'personal data' of individuals, it is defined as a Data Controller for the purposes of the General Data Protection Regulation ("GDPR"). The GDPR places obligations on the way personal data is handled. The employees of the company 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 HR Wallingford 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). HR Wallingford has appointed Graham Leaming, Finance Director as the person with responsibility for data protection compliance within HR Wallingford. He can be contacted via the email address dataprotection@hrwallingford.com. Questions about this policy, or requests for further information, should be directed to him.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information.

"Processing" is any use that is made of data, 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, health, sex life or sexual orientation 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

HR Wallingford processes personal data in accordance with the following data protection principles:

- HR Wallingford processes personal data lawfully, fairly and in a transparent manner HR Wallingford collects personal data only for specified, explicit and legitimate purposes. HR Wallingford also processes personal data for archiving, scientific, research or statistical purposes
- HR Wallingford processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- HR Wallingford keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- HR Wallingford keeps personal data only for the period necessary for processing. HR Wallingford adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Conditions of processing and consent

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

Records of processing activities

HR Wallingford 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 a data subject, 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.

Other rights

Individuals have a number of other rights in relation to their personal data which HR Wallingford will uphold:

- Right to rectify inaccurate data;
- Right to stop processing or erase data that is no longer necessary for the purposes of processing; or if the individual's interests override HR Wallingford's legitimate grounds for processing data (where HR Wallingford relies on its legitimate interests as a reason for processing data);or if processing is unlawful. Individuals can ask HR Wallingford to stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override HR Wallingford's legitimate grounds for processing data.
- Right to 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.
- Rights in relation to automated decision making and profiling – not to be subject to decisions based solely on automated processing. (HR Wallingford does not presently use this method of decision making or profiling)
- Right to 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 HR Wallingford and only when it is processed on the basis of consent or a contract.

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

Data security

HR Wallingford takes the security of personal data seriously. HR Wallingford has internal controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Data security should be undertaken in line with the IS Usage Policy and Security Policy.

Where HR Wallingford engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. Such data sharing must meet one of the conditions of processing (detailed above). Legitimate reasons for transferring data include that it is a legal requirement, or it is necessary for the core business of HR Wallingford. If no other conditions are met then consent will be obtained from the individuals concerned and appropriate privacy notices provided.

International data transfers

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

To safeguard personal data HR Wallingford 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.HR Wallingford 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.

HR Wallingford 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 HR Wallingford keep their personal data up to date. Individuals should let HR Wallingford know if data provided to HR Wallingford changes, for example if an individual moves house or changes his/her bank details. HR Wallingford will update personal data promptly if an individual advises that his/her 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, HR Wallingford relies on individuals to help meet its data protection obligations to staff and other individuals

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside HR Wallingford) who have appropriate authorisation;
- to 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 to remove personal data, or devices containing or that can be used to access personal data, from HR Wallingford's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to 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 HR Wallingford'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 involve personal data GDPR impose a "privacy by design" requirement which HR Wallingford will comply with. Some projects require that a Data Protection Impact Assessment (DPIA) is carried out. This is designed to identify and examine the impact of new initiatives and put in place measures to minimise or reduce risks. 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).

Data breaches

If HR Wallingford 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 within 72 hours of discovery. 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, HR Wallingford will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures HR Wallingford has taken.

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

HR Wallingford 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 HR Wallingford 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

HR Wallingford 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.