

PRIVACY STATEMENT FOR EMPLOYEES

This Policy and Procedure is non-contractual and subject to frequent update. Please do not keep printed copies of this document and check People First for the latest version.

1. PURPOSE

The purpose of this policy is to explain how Kimal collects, uses, stores, and protects personal information relating to its employees, workers, and contractors. As a data controller, we are responsible for ensuring that personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and equivalent local data protection laws in the countries where we employ staff.

This policy ensures that employees understand their rights and the company's obligations in respect of personal data, both during and after employment.

2. DATA COLLECTION

This policy applies to all employees, workers, and contractors of Kimal, whether based in the UK or in other countries where we operate.

It covers all personal data processed through our HR, payroll, and other business systems, including but not limited to:

- **HR and Payroll Systems:** PeopleFirst
- **Benefits Platforms:** Darwin, Fizz Benefits
- **Learning & Development Systems:** PeopleFirst, VinciWorks eLearning
- **IT & Collaboration Tools:** Microsoft suite including (e.g. Outlook, MS Teams, MS SharePoint, Forms) as well as Mimecast
- **ERP Systems:** IFS
- **Other Systems:** Webexpenses, ArrangeMy

This policy applies to all forms of personal data, whether held electronically, in paper files, or other formats.

3. POLICY STATEMENT

Kimal is committed to protecting the privacy and security of personal data. We will:

- Process data lawfully, fairly and transparently.
- Collect data only for valid business purposes.
- Ensure data is adequate, relevant, and limited to what is necessary.
- Keep data accurate and up to date.
- Retain data only as long as necessary for the purposes described or to meet legal obligations.
- Store data securely and restrict access to those with a legitimate business need.

The purposes of the processing of your personal data

We processed your personal data, as your employer. Below, we have set out the categories of employee personal data that we process (which would include the relevant processing of your personal data when you were an employee). As you will see, we have also set out the purposes for processing such personal data.

We may collect and use personal data including but not limited to:

- Personal details (e.g., name, address, date of birth, contact details).
- Employment details (e.g., job title, contract, salary, performance records, attendance).
- Financial information - Payroll and benefits information (e.g., bank details, pensions, healthcare, expenses).
- Special category data where necessary (e.g., health information, race/ethnicity, trade union membership). This personal data may be processed for HR purposes (e.g. to monitor equality and diversity related statistics).
- Limited information on criminal convictions where required for specific roles.

We share your personal data with our colleagues and business associates; governmental, regulatory or other bodies; professional advisors and other third parties where it may be necessary for the purposes outlined above, or other purposes we may inform you of on a case-by-case basis.

- IT systems information - information about your use of our information and communications systems and information obtained through electronic means.
- This personal data may be processed for security reasons (e.g. to monitor and prevent the company being exposed to cyberattacks or other harmful security incidents).
- Family information – this may include information about dependents, next of kin and emergency contact information. This personal data may be processed in case we need to contact such parties (e.g. duty to a medical emergency).
- Information collected throughout the relationship: This may include CCTV or other types of footage, video or audio recordings of meetings or other events you may participate in, and data that is processed to manage your performance. This personal data may be processed for health & safety related reasons (in the case of CCTV); or it may be processed to improve the functioning of the business.
- Information for your security clearances: This may include documentation such as photocopies of passports, or, in limited circumstances, it could information about criminal offences. This personal data may be processed to confirm your identity and protect the security of the business.
- Information about your health: including any medical condition and your medical history, health and sickness records, and accident records.
- This personal data may be processed for HR purposes (e.g. to keep accurate records of leave taken due to medical reasons; comply with any responsibilities that we might have as an employer in respect of any identified health issues (e.g. we may need to provide access to assistance/ support).
- Information we receive from other sources - We may receive information about you from third parties, including:
 - Tax and regulatory authorities such as HMRC – this may be processed in order for us to comply with our legal obligations;
 - Previous employers, recruitment or vetting agencies - this may be processed as part of our recruitment processes to assess your suitability for a role in our company or to carry out security checks; and
 - Colleagues and business associates - this may be processed in order to enable the business to function effectively;
- Other data - which we may notify you of from time to time.
- We collect and use your personal data for different purposes depending on how you interact with us and the services that you supply. Data protection law requires us to have a legal basis to process your personal data for each particular purpose. We will only use your personal data when we have a legal basis for doing so. Most commonly, we will rely on one of the following legal bases:
 - Where we need to perform the contract we are about to enter into or have entered into with you.
 - Where we need to comply with legal/ regulatory requirements.
 - Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
 - Where you have given your consent.

International Transfers

We may transfer your data outside the UK and European Economic Area ("EEA"). However, we will only do so if adequate protection measures are in place in compliance with data protection legislation. We use the following protection measures:

- transferring to Commission approved countries (known as "adequate jurisdictions"); and
- using standard contractual clauses or other mechanisms for transferring personal data internationally that have been approved by the data protection authorities.

How long will your data be stored -

The length of time that we keep your personal data for will vary depending on the nature of the data and purposes for which it is held. For example, we may delete your emails and other business IT accounts promptly upon your departure from our company.

Data from Third Parties

As your employer we may have collected information about you from business counterparts, and governmental bodies such as HMRC.

The existence of automated decision-making, including profiling, - We do not process your personal data for automated decision-making purposes (including profiling).

Employees have legal rights under data protection law, including the right to:

- Request access to their personal information.
- Request correction of inaccurate or incomplete information.

- Request erasure of personal information, where there is no legal or contractual reason for its retention.
- Request restriction of processing in certain circumstances.
- Object to processing based on legitimate interests, including monitoring or reporting.
- Request the transfer of their personal data to another party (data portability).

Where processing is based on consent (for example, optional benefit schemes, diversity monitoring, or the use of photographs in company communications), employees may withdraw that consent at any time. However, where processing is based on legal or contractual requirements (such as payroll, pensions, or tax), the right of erasure or withdrawal of consent will not apply.

Employees who wish to exercise these rights should contact the HR team or Data Protection Officer (DPO).

4. MONITORING AND REVIEW

We may monitor use of company systems (e.g., email, internet, Teams, SharePoint, and other digital platforms) to ensure compliance with our IT and security policies. Monitoring will be proportionate, lawful, and transparent.

This policy will be reviewed regularly and updated as required to reflect changes in law, technology, or business practice. Local retention rules and regulatory requirements will be considered during each review.

5. RESPONSIBILITIES

- Employees are responsible for ensuring that the personal data they provide is accurate and up to date, and for handling any personal data they access in the course of their work in line with this policy.
- Managers are responsible for ensuring their teams understand and comply with this policy.
- HR is responsible for maintaining employee records in compliance with applicable laws and for responding to data subject rights requests.
- IT is responsible for implementing appropriate technical security measures.
- The Data Protection Officer (DPO) oversees compliance with data protection laws, this policy, and acts as the point of contact for queries or complaints.
-

Contact details

Name of DPO: Ametros Group Ltd

Telephone: 0330 223 2246 **Email address:** [dpo@ametrosgroup.com]

Postal address: Ametros Group Ltd, Broadway House, 32-35 Broadstreet, Hereford, England.

Employees may also raise concerns directly with the Information Commissioner's Office (ICO) in the UK or the equivalent data protection regulator in their country of employment.

6. DOCUMENT REVIEW AND CONFIDENTIALITY

This policy will be formally **reviewed at least every two years**, or sooner if required by changes in law or business practice.

All employees are required to maintain the confidentiality of personal data they may access during the course of their work. Unauthorised disclosure or misuse of personal data may result in disciplinary action, up to and including dismissal, and may also constitute a criminal offence.