DATA PROTECTION POLICY

This document sets out Upmo's policy on the protection of information relating to employees, workers, contractors, volunteers and interns (referred to as employees). Protecting the confidentiality and integrity of personal data is a critical responsibility that Upmo takes seriously at all times. Upmo will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

Key Definitions

Data Processing

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Personal Data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers Upmo possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive Personal Data

Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

Privacy Notice

This policy, together with the table of employee data, a copy of which is available from management, constitutes a privacy notice setting out the information Upmo holds about employees, the purpose for which this data is held and the lawful basis on which it is held. Upmo may process personal information without employees' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

If the purpose for processing any piece of data about employees should change, Upmo will update the table of employee data with the new purpose and the lawful basis for processing the data and will notify employees.

Fair Processing of Data

Fair Processing Principles

In processing employees' data, the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

Lawful Processing of Personal Data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, Upmo will use personal information in the following circumstances:

- when it is needed to perform employees' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for Upmo's legitimate interests (or those of a third party) and employees' interests and fundamental rights do not override those interests.

Upmo may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect employees' interests (or someone else's interests); or
- when it is necessary in the public interest or for official purposes.

Lawful Processing of Sensitive Personal Data

Upmo may process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring or in relation to Upmo's occupational pension scheme; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, Upmo may process this type of information where it is needed in relation to legal claims or where it is needed to protect an employee's interests (or someone else's interests) and the employee is not capable of giving consent, or where an employee has already made the information public. Upmo may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;
- information about employees' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;

- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Lawful Processing of Information about Criminal Convictions

Upmo envisages that it will hold information about criminal convictions. Upmo will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out Upmo's obligations. Less commonly, Upmo may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect an employee's interests (or someone else's interests) and the employee is not capable of giving consent, or where the employee has already made the information public. Upmo will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so. Where appropriate, Upmo will collect information about criminal convictions as part of the recruitment process or may require employees to disclose information about criminal convictions during the course of employment.

Consent to Data Processing

Upmo does not require consent from employees to process most types of employee data. In addition, Upmo will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If an employee fails to provide certain information when requested, Upmo may not be able to perform the contract entered into with the employee (such as paying the employee or providing a benefit). Upmo may also be prevented from complying with legal obligations (such as to ensure the health and safety of employees).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, employees may be asked for written consent to process sensitive data. In those circumstances, employees will be provided with full details of the information that sought and the reason it is needed, so that employees can carefully consider whether to consent. It is not a condition of employees' contracts that employees agree to any request for consent.

Where employees have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once Upmo has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law.

Automated Decision Making

Upmo does not envisage that any decisions will be taken about employees using automated means, however employees will be notified if this position changes.

Collection and Retention of Data

Collection of Data

Upmo will collect personal information about employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. Upmo may sometimes collect additional information from third parties including former employers or other background check agencies such as Disclosure Scotland. The table of employee data held within Upmo relates to information which is collected at the outset of employment. From time to time, Upmo may collect additional personal information in the course of job-related activities throughout the period of employment. If Upmo requires to obtain additional personal information, this policy will be updated, or employees will receive a separate privacy notice setting out the purpose and lawful basis for processing the data.

Retention of Data

Upmo will only retain employees' personal information for as long as necessary to fulfil the purposes it was collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the table of employee data appended to this policy.

When determining the appropriate retention period for personal data, Upmo will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether Upmo can achieve those purposes through other means, and the applicable legal requirements. In some circumstances, Upmo may anonymise personal information so that it can no longer be associated with individual employees, in which case Upmo may use such information without further notice to employees. After the data retention period has expired, Upmo will securely destroy employees' personal information.

Data Security and Sharing

Data Security

Upmo has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures are available upon request. Access to personal information is limited to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal information on Upmo's instructions and are subject to a duty of confidentiality. Upmo expects employees handling personal data to take steps to safeguard personal data of employees (or any other individual) in line with this policy.

Data Sharing

Upmo requires third parties to respect the security of employee data and to treat it in accordance with the law. Upmo may share personal information with third parties, for example in the context of the possible sale or restructuring of the business. Upmo may also need to share personal information with a regulator or to otherwise comply with the law.

Upmo may also share employee data with third-party service providers where it is necessary to administer the working relationship with employees or where Upmo has a

legitimate interest in doing so. The following activities are carried out by third-party service providers: payroll, pension administration and IT services.

Employee Rights and Obligations

Accuracy of Data

Upmo will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Employees are under a duty to inform Upmo of any changes to their current circumstances. Where an employee has concerns regarding the accuracy of personal data held by Upmo, the employee should contact their line manager to request an amendment to the data. Employee Rights Under certain circumstances, employees have the right to:

- Request access to personal information (commonly known as a "data subject access request")
- Request erasure of personal information
- Object to processing of personal information where Upmo is relying on a legitimate interest (or those of a third party) to lawfully process it
- Request the restriction of processing of personal information
- Request the transfer of personal information to another party

If an employee wishes to make a request on any of the above grounds, they should contact a member of the SMT in writing. Please note that, depending on the nature of the request, Upmo may have good grounds for refusing to comply. If that is the case, the employee will be given an explanation by Upmo. Data Subject Access Requests Employees will not normally have to pay a fee to access personal information (or to exercise any of the other rights). However, Upmo may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, Upmo may refuse to comply with the request in such circumstances. Upmo may need to request specific information from the employee to help confirm their identity and ensure the right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Compliance with this Policy

Upmo's Responsibility for Compliance

The Board is tasked with overseeing compliance with this policy. If employees have any questions about this policy or how Upmo handles personal information, they should contact a member of the SMT. Employees have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Data Security Breaches

Upmo has put in place procedures to deal with any data security breach and will notify employees and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available from the SMT.

In certain circumstances, Upmo will be required to notify regulators of a data security breach within 72 hours of the breach. Therefore, if an employee becomes aware of a

data security breach it is imperative that they report it to a member of the SMT immediately.

Privacy by Design

Upmo will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as “privacy by design”).

Employees’ Responsibility for Compliance

All employees, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in this policy. Employees should observe, as a minimum, the following rules:

- Employees must observe to the letter any instruction or guidelines issued by Upmo in relation to data protection
- Employees should not disclose personal data about Upmo, colleague or third parties unless that disclosure is fair and lawful, in line with this policy
- Employees must take confidentiality and security seriously, whether the employee considers the information to be sensitive or not
- Any personal data collected or recorded manually which is to be inputted to an electronic system should be inputted accurately and without delay
- Employees must not make any oral or written reference to personal data held by Upmo about any individual except to employees of Upmo who need the information for their work or an authorised recipient
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information
- If an employee is asked by an unauthorised individual to provide details of personal information held by Upmo, the employee should ask the individual to put their request in writing and send it to a member of the SMT. If the request is in writing, the employee should pass it immediately to a member of the SMT.
- Employees must not use personal information for any purpose other than their work for Upmo
- If an employee is in doubt about any matter to do with data protection, they must refer the matter to their line manager immediately
- All files and documents containing confidential information must be locked in suitably secure filing cabinets at all times, other than when being used by staff
- Confidential filing cabinets must be kept locked at all times when the cabinets are not in use. Keys must never be left in the lock of the filing cabinet, and keysafes must never be left unlocked
- Passwords should not be disclosed and should be changed regularly
- Employee or third-party personal data should not be left unsecured or unattended, e.g. on public transport

- Unauthorised use of computer equipment issued by Upmo is not permitted
- Employees must follow Upmo's "clear desk" policy and ensure that all confidential information, whether containing employee or third-party personal data or not, is secured when it is not in use or when the employee is not at work
- Employees may use personal equipment to carry out work but must ensure that devices are password protected, locked when not in use and must not store any employee or third-party personal data locally on their device
- As far as possible, employee or third-party personal data contained in emails and attachments should be anonymised before it is sent by email; and
- Documents containing sensitive information should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately
- Employees should use secure printing where available
- Any documentation which is no longer required should be shredded

Any breach of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment.