Employee Data Protection Policy and Procedure

PURPOSE AND SCOPE

First Mile is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. First Mile takes a privacy by design approach, ensuring that privacy and data protection is a key consideration in any implementation or project as well as throughout its lifecycle. This policy sets out the First Mile'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, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.
First Mile has appointed **James Harland**, **Chief Financial Officer** as the person with responsibility for data protection compliance within First Mile. He can be contacted at **james.harland@thefirstmile.co.uk**. 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

First Mile processes HR-related personal data in accordance with the following data protection principles:

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

First Mile tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.
Where First Mile processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

First Mile will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate. Where any inaccurate or out of date data is found all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.
The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

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. If an individual makes a subject access request, First Mile will tell him/her:

• whether or not his/her 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 the individual;
• to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
• for how long his/her personal data is stored (or how that period is decided);
• his/her rights to rectification or erasure of data, or to restrict or object to processing;
• his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
• whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

First Mile will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise.
To make a subject access request, the individual should send the request to **james.harland@thefirstmile.co.uk**. In some cases, First Mile may need to ask for proof of identification before the request can be processed. First Mile will inform the individual if it needs to verify his/her identity and the documents it requires.
First Mile will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. First Mile will write to the individual within one month of receiving the original request to tell him/her if this is the case.

The personal data will be provided in a structured, commonly used and machine readable form and likely to be either csv or pdf files. The information will be provided free of charge.

Wherever practicable the data and requested by the employee data may be required to transmit the data directly to another organisation if this is technically feasible.

PROFILING

Where the Company uses personal data for profiling purposes, the following shall apply:

Clear information explaining the profiling will be provided, including its significance and If a subject access request is manifestly unfounded or excessive, First Mile is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her 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 can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing (otherwise known as the right to be forgotten);
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- 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 the organisation's legitimate grounds for processing data.
- to ask First Mile to take any of these steps, the individual should send the request to **james.harland@thefirstmile.co.uk**.

DATA PORTABILITY

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual’s consent or for the performance of a contract;
- when processing is carried out by automated means.

First Mile will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data or in the case of numerous or complex requests, it may respond within two months of the date the request is received. First Mile will write to the individual within one the likely consequences:

a) Appropriate mathematical or statistical procedures will be used;
b) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented;
c) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

DATA STORAGE

Personal data collected and held by First Mile is stored in the following ways and in the following locations:

Company data is stored in the Azure data cloud, using O365 and the Azure cloud services which is managed on behalf of First Mile by Infinity Group

Computers & physical records permanently stored in the Company's premises at:

70-71 Wells Street, London, W1T 3QE
38a Minerva Road, Park Royal, London, NW10 6HJ
Vyse St, Hockley, Birmingham, B18 6NF
Unit 5 Broadwell Park, Broadwell Road, Oldbury, B69 4BL

Laptop computers [and other mobile devices] provided by the Company to its employees;
Computers and mobile devices provided by First Mile to employees;

DATA SECURITY

First Mile takes the security of HR-related personal data seriously. First Mile has internal policies and 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.

Where First Mile 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.

The following technical measures are in place within the Company to protect the security of personal data:

• Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
• Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
• Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient [or sent using special delivery via Royal Mail;

• All personal data transferred physically should be transferred in a suitable container marked "confidential";
• All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
• No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without management authorisation;
• Personal data must be handled with care at all times and should not be left unattended or on view;
• Computers used to view personal data must always be locked before being left unattended;
• No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;
• All personal data stored electronically should be backed up;
• All electronic copies of personal data should be stored securely using passwords;
• All passwords used to protect personal data should be changed regularly and should must be secure;
• Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
• All software should be kept up-to-date. Security-related updates should be as soon as reasonably possible after becoming available;
• No software may be installed on any Company-owned computer or device without approval;
• Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Senior Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

ORGANISATIONAL MEASURES

The following organisational measures are in place within the Company to protect the security of personal data:

• All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;
• Only employees and other parties working on behalf of the Company that need access to, and use of personal data in order to perform their work, shall have access to personal data held by the Company;
• All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
• All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
• All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times.
• Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
• The performance of those employees and other parties working on behalf of the Company
• handling personal data shall be regularly evaluated and reviewed;
• All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy.
Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

DATA DISPOSAL

Upon the expiry of the data retention periods set out in this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- Personal data stored electronically (including any and all backups thereof) shall be deleted;
- [Special category personal data stored electronically (including any and all backups thereof) shall be deleted;
- Personal data stored in hardcopy form shall be shredded;
- Special category personal data stored in hardcopy form shall be shredded.

IMPACT ASSESSMENT

Some of the processing that First Mile carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, First Mile will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

DATA BREACHES

If First Mile discovers that there has been a breach of HR-related 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. First Mile will record all data breaches regardless of their effect within the First Mile Data Breach Register.
If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Procedure

All personal data breaches must be reported immediately to First Mile's data protection officer **james.harland@thefirstmile.co.uk**.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including.

INTERNATIONAL DATA TRANSFERS

Employee data may be transferred to countries outside the UK where our chosen information technology provider stores data on servers located outside the UK. We only transfer data for specific and legitimate reasons such as fulfilling a contract.

To ensure your data is transferred lawfully, we rely on Standard Contractual Clauses. Additionally, we implement robust security measures throughout the transfer and storage process, including encryption, access controls, regular security audits.

Please rest assured that your personal information will not be accessible to any organisation or individual outside of the authorised information technology provider

INDIVIDUAL RESPONSIBILITIES

Individuals are responsible for helping First Mile keep their personal data up to date. Individuals should let First Mile know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.
Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, First Mile relies on individuals to help meet its data protection obligations to staff and to customers and clients.

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 the organisation) 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 the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
• 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 the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate

reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

TRAINING

First Mile will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.
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.

This policy has been approved & authorised by:

Bruce Bratley
Chief Executive

Date: 19/01/2025
Review date: 19/01/2026