

Employee/Job Applicant Privacy Notice



Rationale/Purpose	This privacy notice is intended to meet our obligations under the UK General Data Protection Regulation (UK GDPR) and to inform you about how we collect, use, and protect your personal data during and after your employment. We are committed to protecting your privacy and handling your data responsibly.
Who it affects	All staff employed by Imagine Independence People applying for employment with Imagine

1.0 Imagine Independence will collect and process the following categories of personal data:

Category of Data	Examples	Why We Collect It
Personal identifiers	Name, address, phone number, email, date of birth, NI number, Emergency contact details	To manage your employment contract and HR records; to ensure your safety and wellbeing
Recruitment information	CVs, references, right to work checks, qualifications	To assess your suitability for a role and comply with legal obligations
Employment and payroll information	Contract, pay, bank details, tax status, working hours, benefits, holidays	To pay you, manage entitlements, and administer employment-related benefits
Absence records	Sickness absence, annual leave, family leave	To manage leave and support employee wellbeing
Health data (special category)	Fit notes, occupational health reports, disability-related information	To comply with our duty of care and make reasonable adjustments (Equality Act 2010)
Performance and conduct data	Appraisals, disciplinary/grievance records, training	To manage performance, development, and conduct
IT and system usage	Login details, usage logs, access records	To ensure system security and monitor appropriate use of systems

Category of Data	Examples	Why We Collect It
Photographs	ID badges, promotional material,	For site security and (where applicable) marketing or internal communications
CCTV/Ring Doorbell in operation at some premises	CCTV/Ring Doorbell footage	For service user safety monitoring, and ensuring the safety and security of individuals, preventing and detecting crime and protecting property. Such footage may be reviewed and used as evidence in the investigation of allegations of abuse, misconduct or safeguarding concerns. This is done only where it is necessary and proportionate to do so.
Safeguarding and DBS checks	Criminal record information (where lawful and necessary)	To ensure suitability for work in regulated activities and comply with safeguarding laws

1.1 We process your personal data under the following legal bases:

- **Contractual obligation** – to fulfil our obligations under your employment contract
- **Legal obligation** – to comply with employment, tax, health & safety, safeguarding, and care sector laws
- **Legitimate interests** – to manage our operations and workforce efficiently
- **Recognised legitimate interest** – where required for the purpose of crime prevention, security, safeguarding, in the event of emergency, helping other organisations perform their public tasks/official functions
- **Consent** – in specific circumstances (e.g. occupational health referral or publicity photographs)
- **Vital interests** – in emergency situations involving health and safety
- **Public interest** – where required for regulatory, safeguarding, or legal reporting

We process special category data (e.g. health information) under Article 9 of the UK GDPR, including where necessary for carrying out our obligations in employment law and for assessing your working capacity.

1.2 We are the 'data controller' of the personal data we collect and process about you. This means we are responsible for deciding how and why your personal data is used. In some cases, we may also act as a processor, or engage external data processors under appropriate agreements. We rely primarily on our contractual and legal obligations as the lawful basis for processing your employment data. It will also be necessary for us to hold and process this data on the basis of the legitimate interests to safeguard your health, safety and welfare and the health, safety and welfare of your colleagues, clients and third parties in the workplace.

- 1.3 The failure to provide us with the data or to withdraw your consent may impact upon your recruitment, employment or tasks, duties and responsibilities with your role and/or assignment. You should discuss the further impact of this with your manager.
- 1.4 The recipients of your data are us and we anticipate that we may need to share personal data with:
- Internal HR, finance, and management teams
 - Our professional advisers (e.g. legal, payroll, auditors)
 - External IT, training and HR system providers (under data processing agreements)
 - DBS, CQC, HMRC, pension providers, and regulatory or safeguarding bodies
 - Occupational health or medical professionals (with your consent where required)
 - Police, HSE or social services, where necessary to protect health, safety, or comply with safeguarding obligations
 - Tribunals and Courts (e.g. your name, employment details and other personal data which is necessary for the determination of claims where litigation is commenced)
 - Other third parties as part of any investigation into allegations of abuse, misconduct or safeguarding concerns. We may also collect such footage (including from third parties) in investigations of this nature.

Third party recipients are contractually bound to handle data securely and only for specified purposes.

It is not anticipated that there will be any other recipients nor any transfers of data to a third country. Accordingly, it is considered that safeguards for the transfer of data to a third country are not necessary. Should this change, you will be notified.

- 1.5 Your employment data will be kept for the duration of your employment and for a further period thereafter of 6 years. This period has been set for the protection of our organisation throughout your employment and for a period thereafter in the event of any reference requests and employment tribunal claims. If such a claim has been filed, the data will be retained for a period of 6 years following resolution of that claim and for 6 years following the resolution of any further claims. This period has been determined for the protection of the organisation in the event any professional negligence or breach of contract claims in the event we use representation to defend any claims.
- 1.6 Your financial data will be kept for the duration of your employment and for a further period thereafter of 6 years. This period has been set for the protection of our organisation throughout your employment and for a period thereafter in the event of any employment tribunal or breach of contract claims. If such a claim has been filed, the data will be retained for a period of 6 years following resolution of that claim and for 6 years following the resolution of any further claims. This period has been determined for the protection of the organisation under HMRC requirements and in the event any professional negligence or breach of contract claims in the event we use representation to defend any claims.

- 1.7 For safeguarding and care-related records longer retention may apply. DBS and criminal records checks are retained only as long as necessary and in line with Home Office guidance
- 1.8 You have the right to be informed of fair processing information with a view to transparency of data. This statement is intended to fulfil that right
- 1.9 All data will be stored securely online (secure drive/HR/training systems) and in locked personnel or supervisor cabinets

2.0 Access to data and your Rights

- 2.1 Under data protection law, you have rights including:
 - **Access** – to request a copy of the data we hold on you
 - **Rectification** – to request correction of inaccurate data
 - **Erasure** – to request deletion of your data (in certain circumstances)
 - **Restriction** – to limit how we process your data
 - **Objection** – to processing, particularly where we rely on legitimate interests
 - **Data portability** – to request transfer of data to another provider (in limited cases)
- 2.2 **Access:** You have the right to access the information we hold. You should make such a request in writing using the subject access request form, to the Data Protection Officer
- 2.3 **Rectification:** You have the right to request the information we hold is rectified if it is inaccurate or incomplete. You should contact the Data Protection Officer/CEO providing the details of any inaccurate or incomplete data. We will then ensure that this is amended within one month. We may, in complex cases, extend this period to two months.
- 2.4 **Erasure:** You have the right to erasure in the form of deletion or removal of personal data where there is no compelling reason for its continued processing. We have the right to refuse to erase data where this is necessary in the right of freedom of expression and information, to comply with a legal obligation for the performance of a public interest task, exercise of an official authority, for public health purposes in the public interest, for archiving purposes in the public interest, scientific research, historical research, statistical purposes or the exercise or defence of legal claims. You will be advised of the grounds of our refusal should any such request be refused.
- 2.5 **Restriction:** You have the right to restrict our processing of your data where:
 - You are contesting the accuracy of the data until the accuracy is verified.
 - you object to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override your interests.
 - when processing is unlawful, and you oppose erasure and request restriction instead.

- we no longer need the data and you require the data to establish, exercise or defend a legal claim.

You will be advised when we lift a restriction on processing.

2.6 **Objection:** You have the right to object to the following:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

The data collected is not anticipated to fall within the above categories.

2.7 **Data Portability:** You have the right to data portability in that you may obtain and reuse your data for your own purposes across different services, from one IT environment to another in a safe and secure way, without hindrance to usability. The exact method will change from time to time. You will be informed of the mechanism that may be in place should you choose to exercise this right.

2.8 Whilst there is no anticipated automated decision-making relating to the data you provide, you have rights where there is automated decision-making including profiling. We may only do this where it is necessary for the entry into or performance of a contract, authorised by EU or the UK law or based on your explicit consent. Whilst it is not anticipated that this will occur, where it does, we will give you information about this processing, introduce to you simple ways for you to request human intervention or challenge a decision, and carry out regular checks to ensure that our systems are working as intended.

2.9 You have the right to withdraw your consent at any time.

2.10 We encourage you to raise any concerns internally with us first, but you also have the right to lodge a complaint with a supervisory authority such as the Information Commissioner's Office (ICO) or any other of our regulators or accreditors that may regulate or provide accreditations to us from time to time. Please be aware that if you have not first raised your complaint internally with Imagine Independence and awaited conclusion of that process, ICO will most likely direct you back to Imagine Independence before they assess your complaint.