



Data Protection Policy

Introduction

Fruitful Jobs Ltd. ('The Company') takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) where applicable, and other relevant UK data protection legislation. We have a duty to notify you of the information contained in this policy.

This policy applies to data processed regarding current and former employees and workers, job applicants, agency work seekers, agency workers and individual client contacts. If you fall into one of these categories, then you are a 'data subject' for this policy.

You should read this policy alongside your contract of employment, contract for services, Sponsorship Agreement and any other notice we issue to you from time to time in relation to your data.

The Company has registered with the ICO and its registration number is Z216610X.

The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from info@fruitfuljobs.com.

The company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from info@fruitfuljobs.com. We will only hold data for as long as necessary for the purposes for which we collected it.

The Company is a '**data controller**' for your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

The Company will only process personal data where it has a legal basis for doing so.

The Company's Privacy Notice is available on our website.

The Company will review the personal data it holds regularly to ensure it is being lawfully processed and it is accurate, relevant and up to date.

Before transferring information to a third party (e.g., past, current or prospective employers, suppliers, clients, intermediaries or any other third party), the Company will establish that it has a legal basis for making the transfer.

This policy does not form part of your contract of employment or contract for services, if relevant, and can be amended by the Company at any time. It is intended that this policy is fully compliant with UK data protection legislation, including the UK GDPR and the Data Protection Act 2018.

Data Protection Principles

Personal data must be processed in accordance with our '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- not be kept for longer than is necessary for the purposes for which it is processed
- be processed in accordance with the rights of data subjects
- not be transferred outside the United Kingdom unless an appropriate lawful transfer mechanism and any required supplementary safeguards are in place



- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, or your doctor), or it could be created by us. It could be provided or created during the recruitment process, during the course of the contract of employment or contract for services, or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- your contact details and date of birth
- the contact details for your emergency contacts
- information relating to your sex and/or gender (where relevant)
- your marital status and family details
- information about your contract of employment or contract for services, including start and end dates of employment, role and location, working hours, details of promotion, salary/rates of pay (including details of previous remuneration), pension, benefits and holiday entitlement
- your bank details and information in relation to your tax status, including your National Insurance number
- your identification documents, including passport and driving licence, and information in relation to your immigration status and right to work for us
- information relating to disciplinary or grievance/worker complaints and disputes investigations and proceedings involving you (whether or not you were the main subject of those proceedings)
- information relating to your performance and behaviour at work
- training records
- electronic information in relation to your use of IT systems/swipe cards/telephone systems
- your images (whether captured on CCTV, by photograph or video)
- your visa details (where appropriate)
- any other category of personal data which we may notify you of from time to time

How we define special categories of personal data

'**Special categories of personal data**' are types of personal data consisting of information as to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data used for identification purposes
- health
- sex life
- sexual orientation

Information relating to criminal convictions and offences is subject to separate protections under UK data protection law and is not classified as special category personal data.



We may hold and use any of these special categories of your personal data in accordance with the law.

How we define processing

‘**Processing**’ means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage
- adaptation or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination, or otherwise making available
- alignment or combination
- restriction, destruction or erasure

This includes processing personal data that forms part of a filing system, as well as any automated processing.

How will we process your personal data?

The Company will process your personal data (including special category personal data and criminal offence data where applicable) in accordance with UK data protection legislation.

The UK GDPR provides six lawful bases for processing personal data. These lawful bases may apply separately or in combination depending on the purpose of the processing activity. The lawful basis relied upon will depend on the purpose of the processing activity. For most employment and recruitment activities, the Company relies on one or more of the following:

- Compliance with a legal obligation (e.g., real-time information reporting to HMRC)
- The performance of the contract (e.g., processing payroll, monitoring attendance)
- Protecting the legitimate interest of the Company or third party (e.g., collecting information during a disciplinary, grievance, complaints or disputes process, or collecting workplace data to improve workplace performance). You have the right to challenge our legitimate interests and request that we stop this processing. See the section on subject data access rights for further detail.

We can process your personal data for these purposes without specifically informing you or obtaining your consent. We will not use your personal data for an unrelated purpose without informing you of the purpose and the legal basis we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details, we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties, such as paying the correct amount of tax to HMRC.

Privacy by design and default

We are required to demonstrate that privacy considerations are embedded in all our processes and procedures. The Company adopts a data protection by design and default approach. [Data Protection Impact Assessments \(DPIAs\)](#) are undertaken when processing is likely to pose a high risk to individuals' rights and freedoms. DPIAs may also be undertaken where significant changes are made to systems, technologies, processes or working practices.

Examples of the measures that the Company may implement include:

- Data minimisation (i.e., not keeping the data longer than is necessary)
- Pseudonymisation (personal data which cannot be attributed to an individual without additional information. The information must be kept separately and is subject to technical and organisational measures to ensure the individual cannot be identified)
- Anonymisation (processing information so that individuals can no longer be identified)
- Cyber security

Artificial Intelligence and Automated Processing

Data Protection Policy V2 – Last reviewed 01/01/2026 Approved by the Board of Directors



The Company may use technology-assisted recruitment tools, automated assessments, workforce management systems and other technologies to support business operations. Examples may include candidate screening tools, recruitment assessments, workforce scheduling systems, productivity tools and generative AI applications.

Any use of artificial intelligence (AI), profiling or automated processing involving personal data will be subject to appropriate governance, security and oversight measures.

The Company will ensure that:

- There is a lawful basis for processing
- Individuals receive appropriate privacy information
- systems are regularly reviewed for accuracy and fairness
- meaningful human oversight is maintained where decisions may significantly affect individuals
- DPIAs are undertaken where required
- The use of generative AI tools involving personal data is subject to appropriate contractual, security and governance controls

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment, or engagement, and even following the termination of your employment or engagement. For example:

- to decide whether to employ or engage you
- to decide how much to pay you, and the other terms of your contract with us
- to check you have the legal right to work in the UK
- to carry out the contract between us, including, where relevant, its termination
- training you and reviewing your performance
- to decide whether to promote you
- to decide whether and how to manage your performance, absence or conduct
- to carry out a disciplinary or grievance investigation or complaints and disputes procedure in relation to you or someone else
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability
- to monitor diversity and equal opportunities
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others
- to monitor and protect the health and safety of you, our other staff, customers and third parties
- to pay you and provide pension and other benefits in accordance with the contract between us
- paying tax and national insurance
- to provide a reference upon request from another employer
- to pay trade union subscriptions
- monitoring compliance by you, us and others with our policies and our contractual obligations
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us
- to answer questions from insurers in respect of any insurance policies which relate to you
- running our business and planning for the future
- the prevention and detection of fraud or other criminal offences
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure
- to manage visas and the right-to-work process with UKVI, and
- for any other reason which we may notify you of from time to time.

We will process special categories of your personal data (see above) only in certain situations and in accordance with the law. In some circumstances, we may rely on explicit consent. However, in many employment and recruitment situations, the Company will rely on other lawful basis for processing special



category data, such as employment law obligations, health and safety obligations, or the establishment, exercise, or defence of legal claims. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting info@fruitfuljobs.com.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect your vital interests or those of another person, where you/they are physically or legally incapable of giving consent
- where you have made the data public
- where processing is necessary for the establishment, exercise or defence of legal claims
- where processing is necessary for occupational medicine or for the assessment of your working capacity

We may process special category personal data where necessary for the purposes described above and where an appropriate lawful condition applies. In particular, we may use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law, including to make reasonable adjustments and to look after your health and safety
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members
- your visa status

The Company does not normally make decisions that produce legal or similarly significant effects solely by automated means.

Where automated decision-making or profiling is used, the Company will ensure that appropriate safeguards are in place, including the ability to request human review, to express a point of view, and to challenge a decision.

Sharing your personal data

The Company may share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. Examples may include payroll providers, pension providers, IT service providers, recruitment software providers, professional advisers, auditors, insurers, UK Visa and Immigration and regulatory authorities.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are permitted to process your data only for the lawful purpose for which it was shared and in accordance with our instructions.

Personal data may be processed or stored outside the United Kingdom by some of the Company's service providers.

Where personal data is transferred internationally, the Company will ensure that appropriate safeguards are in place in accordance with UK data protection law. These safeguards may include UK adequacy regulations, the International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism.

How should you process personal data for the Company?

Everyone who works for or on behalf of the Company has some responsibility for ensuring that data is collected, stored, and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.



The Company's Directors are responsible for reviewing this policy and for updating the Company's management on the Company's data protection responsibilities and any risks related to data processing. You should direct any questions regarding this policy or data protection to info@fruitfuljobs.co.

The following details the key rules and good practice that apply to everyone in the Company who processes personal data, and you may be subject to monitoring, inspection, and risk assessment to ensure that these are being applied.

- You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should use the data only for the lawful purpose for which it was obtained.
- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes letting us know if your contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Multi-factor authentication (MFA) should be used wherever technically feasible.
- Portable devices containing personal data should be encrypted where appropriate.
- Suspected phishing attempts or cybersecurity incidents must be reported immediately.
- Personal data should only be stored in approved business systems and locations.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the United Kingdom unless authorised and appropriate safeguards are in place.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from the Company's premises without authorisation from your line manager or the [Data Protection Lead, Data Protection Officer (if appointed), or other designated person responsible for data protection compliance].
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from a Director if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also constitute gross misconduct under our disciplinary procedure and could result in your dismissal.

How to deal with data breaches

The Company has technical and organisational measures in place to reduce the risk of personal data breaches and to ensure that incidents can be identified, investigated and managed appropriately. Should a breach of personal data occur (whether in respect of you or someone else), we must take notes and keep evidence of the breach. If the breach is likely to pose a risk to individuals' rights and freedoms, we must also notify the Information Commissioner's Office within 72 hours. The 72-hour reporting period begins when the Company becomes aware of the breach.

The Company maintains a personal data breach register and documents all personal data breaches, regardless of whether notification to the ICO is required.

Where a breach is likely to pose a high risk to individuals' rights and freedoms, we will also take appropriate steps to inform those individuals without undue delay.



If you are aware of a data breach, you must contact a Director immediately and retain any evidence you have related to the breach.

Suspected data breaches will be managed in line with our Data Breach Policy.

Subject access requests

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. Requests may be made verbally or in writing. If you receive such a request, you should forward it immediately to a Director who will coordinate a response.

If you would like to submit an SAR regarding your personal data, you should complete the form on our website. We must respond within one month unless the request is complex or numerous, in which case the response period may be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond.

Data subjects' rights

You have the right to:

- Information about what personal data we process, how and on what basis as set out in this policy.
- Access to your own personal data by way of a subject access request (see above).
- Correct any inaccuracies in your personal data. To do so, you should contact info@fruitfuljobs.com
- Request that we erase your personal data where we were not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected. To do so, you should contact info@fruitfuljobs.com. If you are requesting that your personal data be corrected or erased, or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is being made.
- Object to data processing where we are relying on a legitimate interest to do so, and you think that your rights and interests outweigh our own and you wish us to stop.
- Object if we process your personal data for direct marketing.
- Receive a copy of your personal data and transfer your personal data to another data controller. We will not charge for this and, in most cases, aim to complete it within one month.
- Subject to certain conditions, not to be subject to decisions based solely on automated processing where those decisions produce legal or similarly significant effects.
- Notified of a data security breach concerning your personal data.
- In most situations, we will not rely on your consent as a lawful ground to process your data. If we do, however, request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact info@fruitfuljobs.com. In most situations, we will not rely on your consent as a lawful basis for processing your data.
- Data portability, which allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way, without hindering usability.
- Complain to the Information Commissioner directly.

Further information on your rights, our obligations and available remedies can be found on the ICO website:

<https://ico.org.uk>.

Complaints

If you have concerns about how the Company uses your personal data, you should raise these concerns with info@fruitfuljobs.com.

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Website: <https://ico.org.uk/make-a-complaint/>



Telephone: 0303 123 1113

Review

This policy will be reviewed annually, or sooner if legislation, risks, or best-practice guidance change.