

Our Policy Statement

This Policy and Plan aims to help R Recruitment manage personal data breaches effectively. R Recruitment holds Personal Data about our users, employees, workers, clients, suppliers and other individuals for a variety of business purposes.

R Recruitment is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all Personal Data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

A data breach generally refers to the unauthorised access and retrieval of information that may include corporate and / or personal data. Data breaches are generally recognised as one of the more costly security failures of organisations. They could lead to financial losses, and cause consumers to lose trust in R Recruitment or our clients.

The regulations across the various jurisdictions in which R Recruitment operate require R Recruitment to make reasonable security arrangements to protect the personal data that we possess or control, to prevent unauthorised access, collection, use, disclosure, or similar risks.

Who does it apply to?

This policy applies to current and former R Recruitment employees, workers, volunteers, apprentices and Limited Company Contractors. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1. Policy Principles

1.1. Policy

- 1.1.1. 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 while working for, or on behalf of, the Company.
- 1.1.2. 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 the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

1.2. Data Protection Principles

- 1.2.1. Personal data must be processed in accordance with seven '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; and
 - Be processed securely.
- The controller shall be responsible for, and able to demonstrate compliance with the GDPR.

1.3. How we define personal data

- 1.3.1. '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.
- 1.3.2. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.
- 1.3.3. This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment

process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

1.4. Data we will collect

1.4.1. 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;
- You contact details and date of birth;
- The contact details for your emergency contacts;
- Your gender;
- Your marital status and family details;
- Information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (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 any disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- 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);
- Any other category or personal data which we may notify you of from time to time.

1.5. How we define special categories of data

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

- Your racial or ethnic origin;
- Your political opinions;
- Your religious or philosophical beliefs;
- Your trade union membership;
- Your genetic or biometric data;
- Your health;
- Your sex life and sexual orientation; and
- Any criminal convictions and offences.

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

1.6. How we define processing

1.6.1. 'Processing' means any operation which is performed on personal such as:

- Collection, recording, organisation, structuring or storage;
- Adaption or alteration;
- Retrieval, consultation or use;
- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination; and
- Restriction, destruction or erasure.

1.6.2. This includes processing personal data which forms part of a filing system.

1.7. How we will process your personal data

1.7.1. The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act and GDPR.

1.7.2. We will use your personal data for:

- Performing the contract of employment (or services) in between us;
- Complying with any legal obligation; or

- If it is necessary for our legitimate interests. However, we can only do this if your interests and rights do not override ours. You have the right to challenge our legitimate interests and request that we stop this processing.
- 1.7.3. Our “legitimate interests” for these purposes are the need to:
- Introduce candidates to clients for permanent employment, temporary worker placements or independent professional contract. The exchange of personal data of our candidates and our clients contacts is a fundamental, essential part of this process;
 - Process your data enable us to carry out the employment contract;
 - Gather your data for the purposes of safeguarding your health and safety;
 - Transfer your data intra-group for administrative purposes;
 - Process your data for the purposes of ensuring network and information security; and
 - Protect our legal position in the event of legal proceedings.
- 1.7.4. We may from time to time need to process your sensitive personal data, such as your medical records or other information relating to your health and wellbeing. In that case we will either obtain explicit consent from you or we may consider the processing of that data as being necessary for carrying out our obligations as your employer. That will be assessed on a case by case basis.
- 1.7.5. We will not use your personal data for any purpose different from that for which the data was obtained in the first place without telling you about it and the legal basis that we intend to rely on for processing it.
- 1.7.6. 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 which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer.

1.8. Examples of when we might process your personal data

- 1.8.1. We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).
- 1.8.2. For example (and see section 1.8.5 for the meaning of the asterisks):
- 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 for us;
 - To carry out the contract between us including where relevant, its termination;
 - Training you and reviewing your performance*;
 - To decide whether to promote;
 - To decide whether and how to manage your performance, absence or conduct*;
 - To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
 - To determine whether we need to make a reasonable adjustment 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, clients and others;
 - To monitor and protect the health and safety of you, our other staff, clients 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;
 - 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*;
 - The prevention and detection of fraud and/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*; and
 - For any other reason which we may notify you of from time to time.
- 1.8.3. We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. 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 your local R Recruitment Representative.

1.8.4. We do not need your consent to process special categories of your personal data when we are processing it for the following processes:

- 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; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

1.8.5. We might process special categories of your personal data for the purposes of paragraph 1.8 above which have an asterisk beside them. In particular, we will use this information in relation to:

- Your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities; and
- Your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, adjustments and to look after your health and safety.

1.8.6. We do not take automated decisions about you using your personal data or use profiling in relation to you.

1.9. Sharing your personal data

1.9.1. Sometimes we might share your personal data with our group companies or our contractors and clients to carry out our obligations under our contract with you or for our legitimate interests.

1.9.2. 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 only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions. This could be:

- To pay you via our approved Umbrella Companies;
- To provide you with Benefits and healthcare; and
- To our clients where you may be assigned to assess your suitability for engagement or ongoing assignments.

1.9.3. We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

1.10. Future Employment Interest and Marketing

1.10.1. As a general rule the Company will not send promotional or direct marketing material to you through digital channels such as mobile phones, email and the Internet, without first obtaining your Consent.

1.10.2. The Company shall contact you for future work interests and to continue to offer you work finding services. Should you no longer wish to be considered for work you can tell us by emailing R Recruitment and we shall cease immediately and your details shall be kept on a suppression list with a record of your opt-out decision, rather than being completely deleted.

1.10.3. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

1.11. How should you process personal data for the Company

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

1.11.2. The Company's Compliance Department is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

1.11.3. 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 only use the data for the specified lawful purpose for which it was obtained.

1.11.4. You should not use personal information that you hold in the course of your employment for any reason other than the performance of your employment duties.

1.11.5. You should not share personal data informally.

- 1.11.6. You should keep personal data secure, not on view, and not share it with unauthorised people.
- 1.11.7. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- 1.11.8. You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- 1.11.9. You should use strong passwords.
- 1.11.10. You should lock your computer screens when not at your desk.
- 1.11.11. Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.
- 1.11.12. You should consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- 1.11.13. Do not save personal data to your own personal computers or other devices (See the Company Laptop Policy and USB Storage Devices and Removal Media Policy).
- 1.11.14. Personal data should never be transferred outside the European Economic Area.
- 1.11.15. You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- 1.11.16. You should not take personal data away from Company's premises without authorisation from your line manager.
- 1.11.17. Personal data should be shredded and disposed of securely when you have finished with it.
- 1.11.18. You should ask for help from our Compliance Team if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- 1.11.19. You should immediately report any Data Breaches (such as a loss of personal data or unauthorised access to personal data) to the Compliance Team. For further details please refer to section 1.13 below.
- 1.11.20. 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.
- 1.11.21. 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 amount to gross misconduct under our disciplinary procedure, which could result in your dismissal or termination of contract.

1.12. Training

- 1.12.1. Managers and key members of staff who process personal data will receive training on this policy. Further training will be provided at least every year or whenever there is a substantial change in the law or our policy or procedure.
- 1.12.2. Completion of training is compulsory.

1.13. How to deal with Data Breaches

- 1.13.1. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:
 - Investigate the failure and take remedial steps if necessary
 - Maintain a register of compliance failures
 - Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures
- 1.13.2. Under the GDPR, the Data Protection Representative is legally obliged to notify the Supervisory Authority within 72 hours of the data breach (Article 33). Individuals have to be notified if adverse impact is determined (Article 34). In addition, R Recruitment must notify any affected clients without undue delay after becoming aware of a personal data breach (Article 33).
- 1.13.3. However, R Recruitment does not have to notify the data subjects if anonymised data is breached. Specifically, the notice to data subjects is not required if the data controller has implemented pseudo anonymisation techniques like encryption along with adequate technical and organisational protection measures to the personal data affected by the data breach (Article 34).

1.14. Data Breach Team

- 1.14.1. The Data Breach Team consists of R Recruitment with the support of an external compliance consultancy service.
- 1.14.2. The Data Breach Team should immediately be alerted of any confirmed or suspected data breach via email to lorna@rragency.uk
 - The notification should include the following information, where available:

- 1.14.2..1. Extent of the data breach
- 1.14.2..2. Type and volume of personal data involved
- 1.14.2..3. Cause or suspected cause of breach
- 1.14.2..4. Whether the breach has been rectified
- 1.14.2..5. Measures and processes that the organisation had put in place at the time of the breach
- 1.14.2..6. Information on whether affected individuals of the data breach were notified and if not, when the organisation intends or clarification
- 1.14.3. Where specific information of the data breach is not yet available, R Recruitment should send an interim notification comprising a brief description of the incident.
- 1.14.4. Notifications made by organisations or the lack of notification, as well as whether organisations have adequate recovery procedures in place, will affect supervising authorities decision(s) on whether an organisation has reasonably protected the personal data under its control or possession.

1.15. Subject Access Requests

- 1.15.1. Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the lorna@rragency.uk who will coordinate a response.
- 1.15.2. If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Protection Representative at info@rragency.uk; or via post to Data Protection Representative, R Recruitment Ltd, Suite 1, Ground Floor West, Cardinal Square 10, Nottingham Road, Derby, DE1 3QT. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.
- 1.15.3. 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 to your request.

1.16. Your Data Subject Rights

- 1.16.1. You have the right to information about what personal data we process, how and on what basis as set out in this policy.
- 1.16.2. You have the right to access your own personal data by way of a subject access request (see above).
- 1.16.3. You can correct any inaccuracies in your personal data.
- 1.16.4. You have the right to 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.
- 1.16.5. While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made.
- 1.16.6. You have the right to 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.
- 1.16.7. You have the right to object if we process your personal data for the purposes of direct marketing.
- 1.16.8. You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- 1.16.9. With some exceptions, you have the right not to be subjected to automated decision-making.
- 1.16.10. You have the right to be notified of a data security breach concerning your personal data.
- 1.16.11. 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.
- 1.16.12. If you wish to exercise your rights, or, withdraw your explicit consent, please contact the Data Protection Representative in writing at info@rragency.uk; or via post to Data Protection Representative, R Recruitment Ltd, Unit 4, Stadium Business Centre, Millenium Way, DE24 8HP.

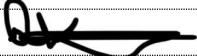
You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

2. Failure to Comply

Where employees are found to be in breach of this policy, they may be subject to disciplinary action up to and including dismissal without payment of notice.

3. Review of Policy

3.1. R Recruitment may review this policy from time to time and when required in line with legislative changes.

Signature:	
Print Name:	R Krawcewicz
Title:	Director