DATA BREACH POLICY

1. Overview

1.1 As an organisation, Just Recruitment Solutions Limited ("**JRS**", "**we**", "**us**, "**our**") values the personal information that is entrusted to us by our candidates, our staff, and other third parties. It is extremely important to us that we uphold that trust in the way in which we handle, use, store and protect personal data.

1.2 We are committed to adopting high standards in our protection of data and in addressing privacy concerns. Not only are we putting in place appropriate technical and security measures, but also ensuring that we have privacy and the protection of data at the heart of our decision-making processes across the organisation.

1.3 We are dedicated to being open and transparent with individuals about how we use and handle their information.

1.4 It is also important to recognise the role of our staff when considering data protection compliance. We will ensure that we provide training to staff who handle personal information as part of their job. Equally, we will treat it as a disciplinary matter if they misuse or fail to take proper care of personal information.

2. General Data Protection Regulation ("GDPR")

2.1 The GDPR will come into effect on **25 May 2018**.

2.2 The GDPR is an EU Regulation, and therefore will have direct effect in the UK, replacing the existing Data Protection Act 1998.

2.3 This policy (and other data protection-related policies operated by JRS) have, where possible, been written with the implementation of GDPR in mind. However, please note that as the GDPR is not yet in force, these documents will need to be reviewed and updated on an ongoing basis to ensure compliance.

2.4 Fundamental to the GDPR is a new standard of accountability. All organisations, including JRS, will be required to demonstrate and evidence how they comply with the data protection principles (as set out further in the Privacy Standard here: [***LINK***]). Compliance with this policy (and our other data protection-related policies) will assist us in doing so.

3. About this policy

3.1 This policy applies to all staff unless otherwise indicated. This policy therefore applies to officers, managers, employees (whether part-time or fixed term), consultants, contractors, agents, casual and temporary or agency staff (collectively referred to as "**Personnel**", "**you**", "**your**").

3.2 This policy may be amended from time to time and Personnel will be directed to certain parts of the policy as and when it is reviewed and updated.

3.3 This policy does not form part of any employee's contract of employment or any other Personnel's contractual terms.

3.4 The directors of JRS will have overall responsibility for data protection compliance within the organisation and for ensuring this policy (together with other data protection-related policies operated by JRS) are adhered to and comply with the relevant legal obligations.

3.5 This policy will be reviewed from time to time by the directors (and the other members of the management team) to ensure that its provisions continue to meet the relevant legal obligations and reflect best practice.

3.6 All those in a management or supervisory role have a specific responsibility to operate in accordance with the provisions set out in this policy and to ensure that all Personnel under their supervision understand the standards of behaviour expected of them, and to take action when behaviour falls below those requirements.

3.7 We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. It is important to note that JRS is exposed to potential fines of up to €20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

3.8 Shaun Pascoe (Director) and Thalia Levers (Office Manager) have been appointed as our data compliance team (the "**Data Compliance Team**"), and are responsible for overseeing data protection compliance, this Data Breach Policy and, as applicable, developing and reviewing any data protection-related policies. The Data Compliance Team can be contacted as follows:

Shaun Pascoe E: shaun@justrecruitmentsolutions.co.uk T: 01603 952785

Thalia Levers E: thalia@justrecruitmentsolutions.co.uk

3.9 Please contact the Data Compliance Team with any questions about the operation of this policy, a data breach or the GDPR in general or if you have any concerns that this policy is not being or has not been followed.

4. Key Dates

4.1 This policy was approved by the director of Just Recruitment Solutions Limited on 11 May 2018.

4.2 This policy became operational on 18 May 2018.

4.3 This policy is next due to be reviewed on 18 May 2019.

5. Recognising a data breach

5.1 A data breach can happen for any number of reasons and it is important that Personnel are able to recognise a data breach and know to whom they should report any suspected or actual data breaches.

5.2 Under the GDPR, the legal definition of a data breach is widely defined:

> "*a breach of security leading to the **accidental or unlawful** destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"

5.3 Examples of when a data breach may occur include the following:

(a) Loss or accidental destruction of files, data or equipment on which data is stored;

(b) Theft of files, data or equipment on which data is stored;

(c) Inappropriate access controls allowing unauthorised use;

(d) Equipment failure;

(e) Unforeseen circumstances such as a fire or flood;

(f) Hacking attack;

(g) Erroneously sending an e-mail to the wrong recipient;

(h) Unauthorised collection or use of personal data;

(i) "Blagging" offences where information is obtained by deceiving the organisation who holds it.

5.4 Under data protection legislation, any of the above may still be a data breach even if JRS can establish that no one has accessed, or can access, the personal data. On that basis, we recommend that a cautious approach is always adopted by Personnel in relation to data breaches. If you have any doubt, the breach should be reported as set out in this policy.

6. Reporting

6.1 It is essential that all Personnel follow the necessary reporting structure in the event of any actual or suspected breach.

6.2 Our reporting structure is as follows:

Personnel must immediately notify the Data Compliance Team of the breach, including details of the nature of the breach, when they discovered it and any steps taken

The Data Compliance Team will assume responsibility for notifying the directors who will, where appropriate, liaise with JRS's legal advisors to determine whether or not to notify the ICO and/or Data Subjects

7. Containment and Recovery

7.1 Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with clients or candidates.

7.2 Our IT providers, EasyPC Limited, will assess and establish whether there is anything that can be done to recover any losses and limit the damage the breach may have caused. This could

involve the use of back up tapes to restore lost or damaged data or ensuring that Personnel recognise when someone tries to use stolen data to access accounts.

8. Notification of breaches

8.1 JRS recognise that informing people and organisations that about a data breach can be an important element in any breach management strategy, and can help to ensure that we are acting transparently with regards to the way that we handle personal data.

8.2 A decision on whom to notify of breaches should be taken in line with the following requirements under the GDPR:

Who to notify	When	Exemption?
ICO / Supervisory Authority *(if JRS is the controller)*	Without undue delay and, where feasible, not later than **72 hours** after becoming aware of it.	No reporting is required if the breach is unlikely to result in a **risk to the rights and freedoms** of natural persons.
Affected Data Subjects *(if JRS is the controller)*	If required, without undue delay however allowing for time where it may be implementing appropriate measures against continuing breaches.	No reporting is required if: a) the breach is unlikely to result in a high risk for the rights and freedoms of data subjects; b) appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or c) reporting would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed).
Clients *(if JRS is the processor)*	Without undue delay	None.

8.3 When notifying the ICO (or other Supervisory Authority) it should be noted that in order to fulfil the reporting requirements notification should include:

(a) description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;

(b) details of information communicated to affected individuals (if any);

(c) the likely consequences of the personal data breach; and

(d) the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

8.4 We will liaise with our legal advisers to determine whether or not a breach notification needs to be made in line with the table at paragraph 8.2 above, and if so, the content of the notification.

8.5 Our legal advisors will also consider with the directors and the Data Compliance Team whether it is appropriate to inform the police of any breach.

8.6 It is important to note that failure to properly notify of the breach may lead to an administrative fine up to **€10,000,000 or up to 2% of the total worldwide annual turnover** of the preceding financial year, whichever is higher. The consequences of failure to notify of a breach could be severe on our business, so all Personnel must ensure to strictly follow the reporting guidelines in this policy. Any failure by Personnel to notify a data breach may be met with disciplinary action.

9. Breach register

9.1 JRS will maintain an internal breach register in order to comply with our obligations under the GDPR. This register will document each breach incident including when the breach occurred, the facts relating to the personal data breach, its potential implications, whether anyone was notified (and if not, why not) and the remedial action taken.

9.2 The ICO may at any time request to review this register to assess how we comply with our data breach notification obligations, so it is crucial to ensure that it is properly maintained.

9.3 The Data Compliance Team will be responsible for holding and maintaining the breach register.

10. Changes to this policy

We reserve the right to change this data breach policy at any time so please check back regularly to obtain the latest copy of this policy. Where appropriate, we will notify you of the changes to this policy as soon as possible.