Privacy and Cookie Policy

Contents

1. Privacy Policy

1.1 Overview

Company Name:	Impact Recruitment ('the Company')
Company Contact details:	Paul Hooper Burlington House East Wing 369 Wellingborough Road Northampton NN1 4EU 01604 239555 Paul.Hooper@ImpactRecruitment.co.uk
Document Title	Privacy and Cookies Policy (including for use on the company website)
Topic:	Data protection
Date:	16.03.20
Version:	2
Reviews:	Impact Recruitment hold quarterly GDPR Reviews and regular training to keep up to date with guidelines and compliance.

The Company is a recruitment business which provides work-finding services to its clients and work-seekers. The Company must process personal data (including sensitive personal data) so that it can provide these services – in doing so, the Company acts as a data controller.

You may give your personal details to the Company directly, such as on an application or registration form or via our website, or we may collect them from another source such as a jobs board. The Company must have a legal basis for processing your personal data. For the purposes of providing you with work-finding services and/or information relating to roles relevant to you we will only use your personal data in accordance with this privacy statement. At all times we will comply with current data protection laws.

1.2 Collection and use of personal data

Purpose of processing and legal basis

The Company will collect your personal data (which may include sensitive personal data) and will process your personal data for the purposes of providing you with work-finding services. This includes for example, contacting you about job opportunities, assessing your suitability for those opportunities, updating our databases, putting you forward for job opportunities, arranging payments to you and developing and managing our services and relationship with you and our clients.

If you have opted-in we may also send you marketing information and news via email/ text. You can opt-out from receiving these at any time by clicking "unsubscribe" when you receive these communications from us.

In some cases we may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws that apply to us. We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

We must have a legal basis to process your personal data. The legal bases we rely upon to offer our work-finding services to you are:

- Where we have a legitimate interest
- Statutory/contractual requirement

- Consent
- Legal Obligation

1.3 Legitimate interest

This is where the Company has a legitimate reason to process your data provided it is reasonable and does not go against what you would reasonably expect from us. Where the Company has relied on a legitimate interest to process your personal data our legitimate interests is/are as follows:

- Managing our database and keeping work-seeker records up to date
- Providing work-finding services to you and our clients
- Contacting you to seek your consent where we need it

1.4 Statutory/contractual requirement

The Company has certain contractual requirements to collect personal data (e.g. to comply with the Conduct of Employment Agencies and Employment Businesses Regulations 2003, immigration and tax legislation, and in some circumstances safeguarding requirements.) Our clients may also require this personal data, and/or we may need your data to enter into a contract with you. If you do not give us personal data we need to collect we may not be able to continue to provide work-finding services to you.

1.5 Consent

This is where the Individual has given clear consent for the Company to process their personal data for a specific purpose. Where the Company has relied on consent to process your personal data may be as follows:

- Sending your CV to our clients
- Providing work-finding services to you and our clients
- Negotiating salary or terms of employment on your behalf

1.6 Legal Obligation

The Company has certain legal obligations to collect personal data (e.g. to comply with the legal obligation to provide employee salary details to HMRC or check right to work documentation.) Our clients may also require this personal data. If you do not give us personal data we need to collect we may not be able to continue to provide work-finding services to you

1.7 Recipient/s of data

The Company will process your personal data and/or sensitive personal data with the following recipients:

- Clients (whom we may introduce or supply you to)
- Payroll service providers who manage payroll on our behalf or other payment intermediaries whom we may introduce you to - Safe Outsourcing and Now Pensions
- Other recruitment agencies in the supply chain
- Candidates' former or prospective new employers that you obtain or provide references to
- The Recruitment and Employment Confederation, UK Government, job boards e.g. CV Library and Broadbean
- Our legal advisers Peninsular
- Our IT and CRM providers – Fuse and Bond Adapt
- Any public information sources and third party organisations that we may use to carry out suitability checks on work-seekers - DVLA
- Government, law enforcement agencies and other regulators e.g. HMRC, Employment Agencies Standards Inspectorate (EASI) GLAA,

- Trade unions;
- Any other organisations an individual asks you to share their data with

1.8 Information to be provided when data collected not from the data subject

Categories of data: The Company has collected the following personal data on you:

Personal data:
- Name, address, mobile no., email
- Date of birth and gender
- CV related information e.g. previous employers, work history
- Bank details and NI number
- Emergency contact details
- Right to work
- Student loan repayments

Sensitive personal data:
- Health information including whether you have a disability
- Criminal conviction

Source of the personal data: The Company sourced your personal data/sensitive personal data:

- From jobs boards, LinkedIn
- You, the work-seeker
- A former employer
- A referee whose details you previously provided to us
- Cookies listed in section 1.12
- Referrals and recommendations

This information did not come from a publicly accessible source.

1.9 Overseas Transfers

The Company will not transfer the information you provide to us to countries outside the European Economic Area ('EEA') for the purposes of providing you with work-finding services. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein.

1.10 Data retention

The Company will retain your personal data only for as long as is necessary for the purpose we collect it. Different laws may also require us to keep different data for different periods of time. For example, the Conduct of Employment Agencies and Employment Businesses Regulations 2003, require us to keep work-seeker records for at least one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.

We must also keep your payroll records, holiday pay, sick pay and pensions auto-enrolment records for as long as is legally required by HMRC and associated national minimum wage, social security and tax legislation. This is currently 3 to 6 years.

Where the Company has obtained your consent to process your personal and sensitive personal data/specify which personal data, we will do so in line with our retention policy [(a copy of which is attached)]. Upon expiry of that period the Company will seek further consent from you. Where consent is not granted the Company will cease to process your personal data and sensitive personal data.

1.11 Your rights

Please be aware that you have the following data protection rights:

- The right to be informed about the personal data the Company processes on you;
- The right of access to the personal data the Company processes on you;
- The right to rectification of your personal data;
- The right to erasure of your personal data in certain circumstances;
- The right to restrict processing of your personal data;
- The right to data portability in certain circumstances;
- The right to object to the processing of your personal data that was based on a public or legitimate interest;
- The right not to be subjected to automated decision making and profiling; and
- The right to withdraw consent at any time.

Where you have consented to the Company processing your personal data and sensitive personal data you have the right to withdraw that consent at any time by contacting Paul Hooper
Burlington House East Wing
369 Wellingborough Road
Northampton
NN1 4EU

01604 239555
Paul.Hooper@Impactrecruitment.co.uk

Please note that if you withdraw your consent to further processing that does not affect any processing done prior to the withdrawal of that consent, or which is done according to another legal basis.

There may be circumstances where the Company will still need to process your data for legal or official reasons. Where this is the case, we will tell you and we will restrict the data to only what is necessary for those specific reasons.

If you believe that any of your data that the Company processes is incorrect or incomplete, please contact us using the details above and we will take reasonable steps to check its accuracy and correct it where necessary.

You can also contact us using the above details if you want us to restrict the type or amount of data we process for you, access your personal data or exercise any of the other rights listed above.

1.12 Cookies

We may obtain data about you from cookies. These are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Cookies also enable us to deliver more personalised content.

The table below explains the cookies we use and why.

Cookie	Name	Purpose
Authentication	RA	We use cookies to identify you when you visit our website and as you navigate our website
Status	RA	We use cookies to help us to determine if you are logged into our website
Personalisation	Ra.tostate, ra.tostateparams, ra.jobsearch	We use cookies to store information about your preferences and to personalise our website for you

Security	__requestverificationtoken	We use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally
Cookie consent	Cookienotice	We use cookies to store your preferences in relation to the use of cookies more generally

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, please refer to our Cookie Policy. [Please note that in a few cases some of our website features may not function if you remove cookies from your browser.]

1.13 Log Files

We use IP addresses to analyse trends, administer the site, track users' movements, and to gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

1.14 Links to external websites

The Company's website may contain links to other external websites. Please be aware that the Company is not responsible for the privacy practices of such other sites. When you leave our site we encourage you to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by the Company's website.

1.15 Sale of business

If the Company's business is sold or integrated with another business your details may be disclosed to our advisers and any prospective purchasers and their advisers and will be passed on to the new owners of the business.

1.16 Data Security

The Company takes every precaution to protect our users' information. Details of this can be found in the chapter Data Security for Microsoft 365 Managed Organisations

Only employees who need the information to perform a specific job (for example, consultants, our accounts clerk or a marketing assistant) are granted access to your information.

The Company uses all reasonable efforts to safeguard your personal information. However, you should be aware that the use of email/ the Internet is not entirely secure and for this reason the Company cannot guarantee the security or integrity of any personal information which is transferred from you or to you via email/ the Internet.

If you share a device with others we recommend that you do not select the "remember my details" function when that option is offered.

If you have any questions about the security at our website, you can email Paul Hooper on

Paul.Hooper@ImpactRecruitment.co.uk

1.17 Changes to this privacy statement

We will update this privacy statement from time to time. We will post any changes on the statement with revision dates. If we make any material changes, we will notify you.

1.18 Complaints or queries

If you wish to complain about this privacy notice or any of the procedures set out in it please contact:

Paul Hooper
Burlington House East Wing
369 Wellingborough Road
Northampton
NN1 4EU

01604 239555
Paul.Hooper@ImpactRecruitment.co.uk

You also have the right to raise concerns with Information Commissioner's Office on 0303 123 1113 or at https://ico.org.uk/concerns/, or any other relevant supervisory authority should your personal data be processed outside of the UK, if you believe that your data protection rights have not been adhered to.

2. *Retention Policy*

Document type	How long to keep for (and source of requirement)
Personnel records	
• Work-seeker records including application form/CV, ID checks, terms of engagement (see also below), details of assignments, opt-out notices and interview notes • Hirer records including client details, terms of business (see below), assignment/vacancy details.	1 year from the last date of providing work-finding services as an Employment Agency or Employment Business (Conduct of Employment Agencies and Employment Businesses Regulations 2003 (Conduct Regulations)) Please note, there is no legal obligation to keep records where you take no action in relation to an application. For full details please pages 16 and 19 to 20 of the REC Guide to the Conduct Regulations.
Terms of engagement with temporary worker and terms of business with clients	6 years in order to deal with any civil action in the form of contractual claim (Limitation Act 1980) (5 years in Scotland). Please note that 6 years is not a minimum legal requirement but is the time period in which a contractual claim can be made. You will still have to establish why it is necessary to keep these records.
Working time records: • 48 hour opt out notice • Annual leave records	2 years from the time they were created
Annual appraisal/assessment records	No specific period – under data protection laws you should only keep records for as long as is necessary.
References	Under data protection laws, only keep records for as long as is necessary. However, the Conduct Regulations require references to be kept for 1 year following the introduction or supply of a work-seeker to a client.
Records held relating to right to work in the UK	2 years after employment or engagement has ended – must not be alterable.
Criminal records checks/ Disclosure Barring checks	There is no longer a 6 month time limit on how long DBS certificates can be kept for. When it comes to handling and storing certificates the new DBS Code requires registered bodies to 'handle all information provided to them by DBS, as a consequence of applying for a DBS product, in line with the obligations under Data protection Act 1998'.
National Minimum Wage documentation: • Total pay by the worker and the hours worked by the worker • Overtime/shift premia;	For HMRC purposes: 3 years after the end of the pay reference period following the one that the records cover (National Minimum Wage Act 1998) Or 6 years (5 in Scotland) in order to show that you have paid at least national minimum

• Any deduction or payment of accommodation; • Any absences eg rest breaks, sick leave, holiday; • Any travel or training during working hours and its length; • Total number of hours in a pay reference period	wage rates if a breach of contract claim is brought against you.
Sickness records – statutory sick pay	Records can be kept in a flexible manner which best suits your business but should be kept for payroll purposes (see below)
Statutory maternity, paternity, adoption pay	3 years from the end of the tax year to which it relates
Pensions auto-enrolment (including auto-enrolment date, joining date, opt in and opt out notices, contributions paid)	6 years except for opt out notices which should be kept for 4 years. For further information please see The Pensions Regulator's detailed guidance for employers.
Gender pay gap reporting	1 year (but the statement must be kept on the Government website and organisation's own website for 3 years).
Company financial records	
VAT	6 years –please see an overview of VAT record keeping on the Gov.uk website.
Company accounts	6 years –please see an overview of running a limited company on the Gov.uk website.
• Payroll information • CIS records	3 years from the end of the tax year – please CIS record-keeping and PAYE record-keeping guidance on the Gov.uk website.
ITEPA (the intermediaries legislation) records	Report due every quarter, to be kept for no less than 3 years after the end of the tax year to which they relate.

3. *Data Security for Microsoft 365 Managed Organisations*

Microsoft 365 is a suite of services and software that enables organisations top operate in an entirely cloud-based, serverless environment. All users, data and devices are managed through a single system, ensuring security is enforced throughout the stack. This document outlines the security and data protection features used in the suite.

3.1 General

Security in Microsoft 365 is based on four principles:

1. Protecting against security threats.
2. Preventing data leaks.
3. Controlling who has access to business information.
4. Reducing risk through privacy and compliance tools.

All services are delivered from Microsoft's Azure datacentres in the UK, which conform to the standards needed by Government, Financial Institutions, the NHS, and internationally recognised security standards to provide a highly secure environment, monitored continuously for threats by the largest team of cybersecurity experts in the world.

3.2 Email

- Email is scanned inbound for malware, spam, and phishing attempts.

- Links in email are converted to “safelinks” which passes the user through a secondary scanning service to check the legitimacy of a link before it’s opened.
- The same thing happens for attachments.
- Sensitive accounts (Directors, Finance) are also subject to further anti-phishing measures.
- Domains and individual addresses can be blacklisted, at organisation and user level.
- Data loss prevention can be deployed to prevent users sending sensitive information (e.g. credit card, national insurance numbers) in bulk.
- Email is backed up at least twice per day to a separate service.
- All email storage is encrypted.
- Access to email is protected by Azure Active Directory (see “User Security”) over encrypted connections.
- All access to email, and every action taken within an email account, is audited, with records kept for 90 days.

3.3 Files

- All files are stored in Microsoft SharePoint, which provides version history, multi-user editing, metadata, web editing, and dual-stage recovery bin, in addition to being backed up.
- Files can be synced via the OneDrive application to both Windows and mobile devices, to enable access from anywhere.
- Synced files are encrypted on the device and managed by security policies.
- Conditional access can be used to restrict file syncing to managed devices only.
- Data loss prevention can be used for SharePoint files in the same way as email.
- Access to SharePoint is protected by Azure Active Directory (see “User Security”) over encrypted connections.
- All access to SharePoint, and every action taken within SharePoint, is audited, with records kept for 90 days.

3.4 Managed Windows Computers

- Windows Computers are registered within Microsoft 365 and managed over the internet.
- All configuration settings and installed applications are applied through policies.
- Security settings, which include full disk encryption, antivirus configuration and lock screen timeouts, are applied through policies and assessed for non-compliance.
- Non-compliant devices may be prevented from accessing company resources (email and files)
- Managed devices can be remote-wiped, reset and refreshed.
- All Windows devices have their antivirus and firewall switched on.
- Windows Updates are continuously applied.
- The use of PIN/Biometric logins (which exist on the device only) is encouraged to prevent “over the shoulder” gaining of credentials, which could then be used on another device.

3.5 Mobile Devices

- Mobile devices can be fully managed (as Windows devices are – see above) or BYOD, in which case only the company application data is managed.
- In both cases, the mobile device is configured to meet a minimum security standard, before access to company data is granted – i.e. a secure PIN, full encryption, no jailbroken devices.
- On BYOD devices, only the application partition is wiped.

3.6 Connectivity

- All connections to Microsoft 365 Services are encrypted using TLS 1.2 and 256 bit keys.
- Conditional access can be used to restrict access from only certain locations (e.g. organisation offices) or managed devices that are fully compliant.

3.7 User Security

- All user credentials are stored in Azure Active Directory, which provides a single authority for all services.

- Each user has a unique set of credentials that is managed by the user themselves, i.e. it can be reset be them at any time.
- Users can also be set up with Multi-Factor authentication (i.e. password + device) to further increase security. This is recommended for sensitive accounts (administrators/directors/finance).
- Passwords must be changed at least every 60 days.
- Logins are monitored for anomalies such as unusual sign-in locations.
- Accounts are locked out if too many attempts are made to sign-in with an incorrect password.
- User accounts are securely stored within the OS on managed machines, reducing the number of logins needed to Microsoft 365 services (Single-Sign-On).
- All account actions are audited with records kept for 90 days.

4. Cookie Policy

4.1 Introduction

4.11 We are committed to safeguarding the privacy of our website visitors and service users

4.12 This policy applies where we are acting as a data controller with respect to the personal data of our website visitors and service users; in other words, where we determine the purposes and means of the processing of that personal data.

4.13 By using our website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy.

4.14 In this policy, "we", "us" and "our" refer to Impact Recruitment Services.

4.2 How we use your personal data

In this Section 4.2 we have set out:

(a) the general categories of personal data that we may process;
(b) in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
(c) the purposes for which we may process personal data; and
(d) the legal bases of the processing.

4.21 We may process data about your use of our website and services ("usage data"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analysing the use of the website and services. The legal basis for this processing is our legitimate interests, namely monitoring and improving our website and services.

4.22 We may process your account data ("account data"). The account data may include your name and email address. The source of the account data is you or your employer. The account data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business.

4.23 We may process your information included in your personal profile on our website ("profile data"). The profile data may include your name, address, telephone number, email address, profile pictures, gender, date of birth, relationship status, interests and hobbies, educational details and employment details. The profile data may be processed for the purposes of enabling and monitoring your use of our website and services. The legal basis for this processing is our legitimate interests, namely for the purpose of providing work-seeking services to you.

4.24 We may process your personal data that are provided in the course of the use of our services ("service data").The service data may include name, address, telephone number, email address, profile pictures, gender, date of birth, relationship status, interests and hobbies, educational details and employment details. The source of the service data is you or your employer. The service data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is our legitimate interests, namely for the purpose of providing work-seeking services to you.

4.25 We may process information that you post for publication on our website or through our services ("publication data"). The publication data may be processed for the purposes of enabling such publication and administering our website and services. The legal basis for this processing is our legitimate interests, namely for the purpose of providing work-seeking services to you.

4.26 We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("notification data"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is consent.

4.27 We may process information contained in or relating to any communication that you send to us ("correspondence data"). The correspondence data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website contact forms. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business and communications with users.

4.28 We may process any of your personal data identified in this policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

4.29 We may process any of your personal data identified in this policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

In addition to the specific purposes for which we may process your personal data set out in this Section 4.2, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

Please do not supply any other person's personal data to us, unless we prompt you to do so.

4.3 Providing your personal data to others

4.31 We may disclose your personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.

4.32 We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

4.33 In addition to the specific disclosures of personal data set out in this Section 3, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure

is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

4.4 Retaining and deleting personal data

This Section 4.4 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

4.41 Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

4.42 We will retain your personal data as follows:

(a) personal data category or categories will be retained for a minimum period of 1 year following the last date of providing work finding services as an Employment Agency or Employment Business, and for a maximum period of 6 years following the last date of providing work finding services as an Employment Agency or Employment Business. The type of personal data category or categories will determine the length the record must be kept for and will be based on current guidance, legislation and Law.

4.43 In some cases it is not possible for us to specify in advance the periods for which your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria:

(a) the period of retention of personal data will be determined based on document type and the current guidance from the Government with regards to VAT,PAYE Records and Limited Company, REC (our Governing Body), the Conduct of Employment Agencies and Employment Business Regulations 2003 ((Conduct Regulations)), the Limitation Act 1980, the DBS Code, National Minimum Wage Act 1998, The Pensions Regulator, and in accordance with current Data Protection Laws.

4.44 Notwithstanding the other provisions of this Section 6, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

4.5 Security of personal data

4.51 We will take appropriate technical and organisational precautions to secure your personal data and to prevent the loss, misuse or alteration of your personal data.

4.52 We will store all your personal data on secure servers, personal computers and mobile devices, and in secure manual record-keeping systems.

4.53 The following personal data will be stored by us in encrypted form: your name, contact information, password(s).

4.54 Data relating to your enquiries and financial transactions that is sent from your web browser to our web server, or from our web server to your web browser, will be protected using encryption technology.

4.55 You acknowledge that the transmission of unencrypted (or inadequately encrypted) data over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

4.56 You should ensure that your password is not susceptible to being guessed, whether by a person or a computer program. You are responsible for keeping the password you use for accessing our website confidential and we will not ask you for your password (except when you log in to our website).

4.6 Amendments

4.61 We may update this policy from time to time by publishing a new version on our website.

4.62 You should check this page occasionally to ensure you are happy with any changes to this policy.

4.63 We may notify you of changes to this policy by email or through the private messaging system on our website.

4.7 Your rights

In this Section 8, we have summarized the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

4.71 Your principal rights under data protection law are:

(a) the right to access;

(b) the right to rectification;

(c) the right to erasure;

(d) the right to restrict processing;

(e) the right to object to processing;

(f) the right to data portability;

(g) the right to complain to a supervisory authority; and

(h) the right to withdraw consent.

4.72 You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.

4.73 You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

4.74 In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

4.75 You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task

carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

4.76 You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.

You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

4.77 To the extent that the legal basis for our processing of your personal data is:

(a) consent; or

(b) that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

4.78 To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

4.79 You may exercise any of your rights in relation to your personal data by written notice to us, in addition to the other methods specified in this Section 8.

4.8 Third party websites

4.81 Our website includes hyperlinks to, and details of, third party websites.

4.82 We have no control over, and are not responsible for, the privacy policies and practices of third parties.

Personal data of children
4.83 Our website and services are targeted at persons over the age 16.

4.84 If we have reason to believe that we hold personal data of a person under that age in our databases, we will delete that personal data.

4.9 Updating information

4.91 Please let us know if the personal information that we hold about you needs to be corrected or updated.

4.10 Cookies

4.101 A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

4.102 Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

4.103 Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

Cookies that we use

4.111 We use cookies for the following purposes:

(a) authentication - we use cookies to identify you when you visit our website and as you navigate our website (cookies used for this purpose are: RA);

(b) status - we use cookies to help us to determine if you are logged into our website (cookies used for this purpose are: RA);

(c) personalisation - we use cookies to store information about your preferences and to personalise our website for you (cookies used for this purpose are: RA.toState, RA.toStateParams, RA.jobSearch);

(d) security - we use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally (cookies used for this purpose are: __RequestVerificationToken);

(e) cookie consent - we use cookies to store your preferences in relation to the use of cookies more generally (cookies used for this purpose are: cookieNotice).

Cookies used by our service providers

Our service providers use cookies and those cookies may be stored on your computer when you visit our website.

We use Google Analytics to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: https://www.google.com/policies/privacy/. The relevant cookies are: _ga, _gid,_gat

4.12 Managing cookies

Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

(a) https://support.google.com/chrome/answer/95647?hl=en (Chrome);

(b) https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences (Firefox);

(c) http://www.opera.com/help/tutorials/security/cookies/ (Opera);

(d) https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies (Internet Explorer);

(e) https://support.apple.com/kb/PH21411 (Safari); and
(f) https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy (Edge).

Blocking all cookies will have a negative impact upon the usability of many websites.

If you block cookies, you will not be able to use all the features on our website.

Our details

This website is owned and operated by Impact Recruitment Services.

We are registered in England and Wales under registration number 4426909, and our registered office is at 7 Billing Road, Northampton NN1 5AN.

Our principal place of business is at 369 Wellingborough Road, Burlington House East Wing, Northampton NN1 4EU.

You can contact us:

(a) by post, to the postal address given above;
(b) using our website contact form;
(c) by telephone, on the contact number published on our website from time to time; or
(d) by email, using the email address published on our website from time to time.

4.13 Data protection registration

We are registered as a data controller with [the UK Information Commissioner's Office].

Our data protection registration number is ZA113058.

4.14 Data protection officer

Our data protection officer's contact details are:
Paul Hooper, 369 Wellingborough Road, Burlington House East Wing, Northampton NN1 4EU;

paul@impactrecruitment.co.uk;
01604 239555

5. Adapt

The Company store candidate and client data on Adapt, which is Erecruit recruitment software that files and stores information such as contact details, CV's and records. All the data stored is patched against vulnerabilities and regular vulnerability tests are conducted on external facing IP addresses. Adapt have the most up-to-date level of anti-virus available for the operating system, application and manufacturer, have network level intrusion detection/prevention and firewalls in place and is kept up-to-date in line with best practices.

Adapt undertake regular information risk assessments for target environments (e.g. critical business environments, business processes, business applications) in a rigorous and consistent manner, using a structured methodology. They have a detailed written incident management plan to manage security incidents, including the identification, response, recovery and post-implementation review of data breaches in place and in line with internal processes and ISO standards.

Independent checks are carried out to ensure customer data has not been accessed, manipulated or extracted, unless required for a particular task.

All information is processed, stored and backed up within the European Economic Area only.

There are risk assessments of threats in respect of backed-up customer data, from the point of back-up creation, through transit, to the ultimate place of storage. Due diligence is carried out on any third parties that handle backed-up customer data, so that the supplier has a good understanding of how it is secured and accessed, and failover capabilities are in place and regularly tested.

All the data stored is kept in line with the Company Retention Policy.