

Data Protection Policy

1. Introduction

At **Icon People Recruitment Ltd**, safeguarding personal information is a fundamental part of how we conduct our business. We are committed to collecting, using, storing, and protecting personal data responsibly and in accordance with all applicable data protection legislation.

This policy explains how the Company manages personal information relating to employees, workers, job applicants, agency workers, work seekers, former employees, clients, and other individuals whose personal information we process during the course of our business activities.

Our organisation complies with the requirements of the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. These laws set out how personal information must be handled and the rights individuals have regarding their personal data.

This policy should be read alongside your employment contract, worker agreement, service agreement, Company Privacy Notice, Data Security Policy, Data Retention Policy, and any other documents relating to the processing of personal information.

Icon People Recruitment Ltd is registered with the **Information Commissioner's Office (ICO)** under registration number **ZC1781541**.

The Company has implemented appropriate technical and organisational measures to ensure personal information is protected against unauthorised access, accidental loss, misuse, alteration, or disclosure.

Any questions regarding this policy or the way your personal information is processed should be directed to:

GDPR Team

Icon People Recruitment Ltd
11–15 Guildhall Lane
Leicester
LE1 5FQ
United Kingdom
Email: info@iconpeoplerecruitment.uk

Personal information will only be retained for as long as necessary to fulfil the purpose for which it was collected or where required by law. Once the applicable retention period expires, the information will be securely deleted or destroyed.

For the purposes of data protection legislation, **Icon People Recruitment Ltd acts as the Data Controller**. This means the Company decides how and why personal information is collected, processed, stored, and shared.

The Company will only process personal information where there is a valid legal basis to do so. We also regularly review the information we hold to ensure it remains accurate, relevant, up to date, and necessary for the purposes for which it is processed.

Before any personal information is disclosed to external organisations—including clients, suppliers, service providers, prospective employers, or other authorised third parties—the Company will ensure that an appropriate lawful basis exists for sharing that information.

This policy is provided for guidance and compliance purposes only. It does not form part of any contract of employment or engagement and may be reviewed or updated by the Company whenever necessary to reflect changes in legislation, regulatory guidance, or business requirements.

2. Data Protection Principles

Icon People Recruitment Ltd is committed to processing all personal data in a responsible, transparent, and lawful manner. Every employee, worker, contractor, and any individual acting on behalf of the Company is expected to comply with these principles whenever personal information is collected, used, stored, shared, or disposed of.

The Company will ensure that all personal data is handled in accordance with the following principles established under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Lawfulness, Fairness and Transparency

Personal information will only be processed where there is a valid legal basis for doing so. Individuals will be provided with clear information explaining how their personal data is collected, why it is required, and how it will be used. The Company will always process personal information honestly, fairly, and transparently.

Purpose Limitation

Personal data will only be collected for specific, legitimate, and clearly defined business purposes. Once the information has been collected, it will not be used for unrelated purposes unless permitted by law or where an appropriate legal basis exists.

Data Minimisation

The Company will only collect and retain personal information that is directly relevant and necessary for the purpose for which it is being processed. Unnecessary or excessive personal data will not be requested, stored, or processed.

Accuracy

Reasonable steps will be taken to ensure that all personal information remains accurate, complete, and up to date. Where inaccurate or outdated information is identified, it will be corrected or securely removed as soon as reasonably practicable.

Individuals are encouraged to notify the Company promptly of any changes to their personal details to help maintain accurate records.

Storage Limitation

Personal information will not be retained indefinitely. Data will only be kept for as long as it is required to fulfil the purpose for which it was collected, to meet contractual obligations, or to satisfy legal and regulatory requirements.

Once the applicable retention period has expired, the Company will securely delete, destroy, or anonymise the information in accordance with its Data Retention Policy.

Integrity and Confidentiality

The Company will implement appropriate technical and organisational measures to protect personal information from unauthorised access, accidental loss, misuse, alteration, disclosure, or destruction.

Security measures may include, but are not limited to:

- Access controls and user permissions.
- Password-protected systems.
- Encryption where appropriate.
- Secure storage of paper and electronic records.
- Regular monitoring and cyber security measures.
- Staff training on data protection responsibilities.

Only authorised individuals who require access for legitimate business purposes will be permitted to process personal data.

International Transfers

Personal data will not be transferred outside the United Kingdom or countries providing an adequate level of data protection unless appropriate legal safeguards have been implemented in accordance with applicable data protection legislation.

Where international transfers become necessary, the Company will ensure that suitable contractual or legal protections are in place before any personal information is transferred.

Accountability

Icon People Recruitment Ltd accepts full responsibility for complying with data protection legislation and maintaining appropriate records to demonstrate that compliance.

The Company regularly reviews its policies, procedures, and processing activities to ensure that personal information continues to be managed in accordance with legal requirements and recognised best practices.

All individuals working for or on behalf of the Company are responsible for supporting these principles and ensuring that personal data is handled securely, confidentially, and in accordance with this policy at all times.

3. Definitions of Personal Data, Special Category Data and Processing

3.1 Personal Data

For the purposes of this policy, **personal data** refers to any information that identifies, or could reasonably be used to identify, a living individual, either on its own or when combined with other information available to the Company.

Personal data may exist in electronic records, paper documents, emails, photographs, audio or video recordings, or any other format in which information is stored.

The Company may obtain personal information directly from the individual concerned, from third parties where legally permitted, or generate such information during the course of recruitment, employment, business operations, or the provision of recruitment services.

Examples of personal data that the Company may collect and process include, but are not limited to:

- Personal identification details, including name, date of birth and contact information.
- Recruitment records such as application forms, CVs, interview notes, references, qualifications, licences, certifications and professional memberships.
- Emergency contact details.
- Gender and other personal profile information where required.

- Employment or engagement records, including job title, department, location, working hours, contractual terms, salary, benefits, pension arrangements, promotions and employment history.
- Payroll and financial information, including bank account details, National Insurance number and tax-related information.
- Identity verification documents such as passports, driving licences and right-to-work documentation.
- Immigration and visa information where required for legal compliance.
- Attendance, absence and leave records.
- Performance reviews, training records and career development information.
- Records relating to disciplinary matters, grievances, complaints, investigations or dispute resolution procedures.
- Information concerning workplace conduct and professional behaviour.
- Electronic usage data generated through Company systems, including computer networks, email services, access control systems, telephones and swipe card records.
- CCTV recordings, photographs and video images used for legitimate business, security or identification purposes.
- Any additional personal information that is reasonably required to fulfil legal, contractual or operational obligations.

The categories of personal data processed may vary depending on an individual's relationship with the Company.

3.2 Special Category Personal Data

Certain types of personal information require a higher level of protection because they are considered particularly sensitive under data protection legislation. These are known as **Special Category Personal Data**.

This may include information relating to:

- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Political opinions.
- Trade union membership.

- Genetic information.
- Biometric data used for identification.
- Physical or mental health.
- Sexual orientation or sex life.

Where permitted by law, the Company may also process information relating to criminal convictions or offences where this is necessary for recruitment, safeguarding, regulatory compliance or other legitimate legal purposes.

The Company will only process Special Category Personal Data where an appropriate lawful condition exists under the UK GDPR and the Data Protection Act 2018. Additional safeguards will always be applied to protect this information.

3.3 Meaning of Processing

The term **processing** refers to any activity carried out in relation to personal data, whether performed manually or by automated systems.

Processing includes, but is not limited to:

- Collecting or obtaining information.
- Recording or entering data into Company systems.
- Organising, classifying or storing information.
- Updating, amending or correcting records.
- Retrieving, viewing or consulting personal data.
- Using information for legitimate business purposes.
- Sharing or disclosing information with authorised third parties.
- Combining information from different sources.
- Restricting access where appropriate.
- Archiving records.
- Deleting, anonymising or securely destroying personal data.

These activities apply regardless of whether the information is stored electronically, on paper, within filing systems or by any other secure method.

All processing carried out by Icon People Recruitment Ltd will be undertaken in accordance with the principles of lawfulness, fairness, transparency, security and accountability as required by applicable UK data protection legislation.

4. Processing of Personal Data

4.1 Lawful Processing

Icon People Recruitment Ltd will only collect, use, store, or otherwise process personal data where there is a valid legal basis under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Company is committed to ensuring that all processing activities are carried out fairly, lawfully, transparently, and only for legitimate business purposes.

Depending on the circumstances, personal data may be processed under one or more of the following lawful bases:

Compliance with Legal Obligations

The Company may process personal information where it is necessary to meet legal or regulatory requirements imposed upon the business.

Examples include:

- Meeting HM Revenue & Customs (HMRC) reporting obligations.
- Verifying an individual's right to work in the United Kingdom.
- Maintaining statutory employment records.
- Complying with health and safety legislation.
- Preventing fraud and financial crime.
- Responding to lawful requests from regulatory bodies or government authorities.

Performance of a Contract

Processing may also be necessary to fulfil contractual obligations between the Company and an employee, worker, candidate, client, supplier or other business partner.

This may include activities such as:

- Recruitment and onboarding.
- Managing employment or worker contracts.
- Processing salaries, wages and other payments.

- Administering pensions and employee benefits.
- Recording attendance and working hours.
- Managing holiday entitlement and leave.
- Delivering recruitment and workforce services to clients.
- Providing ongoing employment administration.

Without certain personal information, the Company may be unable to fulfil its contractual responsibilities.

Legitimate Business Interests

Where appropriate, the Company may process personal data to support its legitimate business interests, provided those interests do not override the rights and freedoms of the individual concerned.

Examples include:

- Protecting Company property and business assets.
- Maintaining IT and network security.
- Investigating disciplinary matters, grievances or complaints.
- Managing disputes and legal claims.
- Monitoring service quality and business performance.
- Preventing fraud or misuse of Company systems.
- Improving operational efficiency.
- Ensuring compliance with internal policies and procedures.

Where processing is based on legitimate interests, the Company will carefully assess the impact on individuals and ensure that their rights remain appropriately protected.

Individuals have the right to object to processing carried out under this lawful basis where permitted by law.

4.2 Purpose of Processing

Personal information will only be processed for purposes that are lawful, relevant and necessary to the Company's business operations.

These purposes may include:

- Recruiting suitable candidates.
- Managing employment relationships.
- Providing recruitment and workforce solutions.
- Maintaining accurate personnel records.
- Processing payroll and financial transactions.
- Administering employee benefits.
- Delivering training and professional development.
- Monitoring attendance, performance and conduct.
- Protecting health, safety and workplace security.
- Managing client relationships.
- Meeting legal and regulatory obligations.
- Defending or pursuing legal claims where necessary.
- Supporting the efficient operation and future development of the business.

Personal information will not be used for purposes that are incompatible with the original reason for which it was collected unless required or permitted by law.

4.3 Special Category Personal Data

Where the Company processes Special Category Personal Data, this will only take place where an additional lawful condition under the UK GDPR and the Data Protection Act 2018 has been satisfied.

Such processing may be necessary for purposes including:

- Complying with employment legislation.
- Assessing fitness for work.
- Managing sickness absence.
- Providing occupational health support.
- Making reasonable workplace adjustments.
- Monitoring equality, diversity and inclusion.
- Safeguarding employees, workers and clients.
- Establishing, exercising or defending legal claims.

Where consent is relied upon, it will be obtained clearly and voluntarily. Individuals may withdraw their consent at any time, although this will not affect the lawfulness of any processing carried out before consent was withdrawn.

4.4 Failure to Provide Personal Information

Certain personal information is essential for the Company to meet its contractual and legal responsibilities.

If an individual chooses not to provide information that is reasonably required, the Company may be unable to:

- Complete the recruitment process.
- Offer employment or engagement.
- Process salary or other payments.
- Verify identity or right to work.
- Meet legal or regulatory obligations.
- Deliver certain employment-related benefits or services.

Where this occurs, the Company will explain the potential consequences and, where possible, discuss alternative solutions.

4.5 Processing for New Purposes

If the Company intends to process personal information for a purpose that differs significantly from the reason for which it was originally collected, individuals will be informed before the new processing begins.

Where required by law, the Company will identify the appropriate lawful basis and provide any additional privacy information necessary to ensure transparency and compliance with applicable data protection legislation.

5. Privacy by Design and Information Security

5.1 Our Commitment

Icon People Recruitment Ltd recognises that protecting personal information is an essential part of its business operations. Data protection is considered at every stage of our processes, systems, and services to ensure that personal information is handled securely, lawfully, and responsibly.

The Company follows the principle of **Privacy by Design and by Default**, meaning that privacy and data protection requirements are incorporated into all business activities from the outset rather than being added later.

Whenever new systems, technologies, policies, procedures, or business processes are introduced or significantly changed, appropriate data protection considerations will be assessed before implementation.

5.2 Data Protection Impact Assessments (DPIAs)

Where a new project, system, or process is likely to present a higher risk to individuals' privacy rights, the Company will carry out a **Data Protection Impact Assessment (DPIA)** before processing begins.

The purpose of a DPIA is to:

- Identify potential privacy and data protection risks.
- Evaluate the necessity and proportionality of the proposed processing.
- Assess the impact on individuals' rights and freedoms.
- Determine appropriate measures to reduce or eliminate identified risks.
- Demonstrate compliance with applicable data protection legislation.

The Company will review these assessments whenever significant operational or legal changes occur.

5.3 Data Minimisation

The Company will only collect and retain personal information that is necessary for specific business purposes.

To support this principle, we will:

- Collect only information that is relevant and proportionate.
- Avoid requesting excessive or unnecessary personal data.
- Regularly review stored information to ensure it remains appropriate.
- Securely delete or anonymise information that is no longer required.

This approach reduces privacy risks while ensuring compliance with legal obligations.

5.4 Information Security Measures

Appropriate technical and organisational safeguards are maintained to protect personal information from accidental loss, unauthorised access, misuse, disclosure, alteration, or destruction.

Depending on the nature of the information being processed, these safeguards may include:

- Role-based access controls to limit access to authorised personnel only.
- Strong password requirements and secure authentication procedures.
- Encryption of personal data where appropriate.
- Secure computer networks protected by firewalls and anti-malware software.
- Regular software updates and security patch management.
- Monitoring of Company systems to identify potential security threats.
- Secure storage of paper records within restricted-access areas.
- Controlled disposal of confidential documents and electronic media.
- Staff training on information security and data protection responsibilities.

These measures are reviewed regularly to ensure they remain effective against emerging security risks.

5.5 Cyber Security

Maintaining effective cyber security is a key part of protecting personal information.

The Company will implement reasonable security measures designed to safeguard its IT infrastructure, including protection against cyber attacks, malware, phishing, ransomware, unauthorised system access, and other security threats.

Employees, workers, and anyone acting on behalf of the Company are expected to follow all IT security policies and immediately report any suspected cyber security incident or vulnerability.

5.6 Continuous Monitoring and Improvement

Data protection and information security are ongoing responsibilities.

The Company will regularly review its policies, procedures, systems, and security controls to ensure they remain compliant with the UK General Data Protection

Regulation (UK GDPR), the Data Protection Act 2018, and recognised industry best practices.

Where improvements are identified, appropriate corrective actions will be implemented to strengthen the protection of personal information and reduce operational risk.

Through continuous monitoring, staff awareness, and regular policy reviews, Icon People Recruitment Ltd aims to maintain a high standard of information security while ensuring the confidentiality, integrity, and availability of all personal data processed by the Company.

6. Sharing Personal Data

6.1 Our Approach to Sharing Information

Icon People Recruitment Ltd recognises the importance of maintaining the confidentiality and security of personal information. Personal data will only be shared where there is a legitimate business requirement, a legal obligation, or another lawful basis under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Company does not disclose personal information unnecessarily and always seeks to ensure that any sharing of data is appropriate, secure, and proportionate to the purpose for which it is required.

6.2 Who We May Share Personal Data With

Where necessary, personal information may be shared with authorised third parties in connection with the Company's business activities.

These may include:

- Clients and prospective clients for recruitment and placement purposes.
- Payroll providers and pension administrators.
- Professional advisers, including solicitors, accountants and auditors.
- Government departments, regulatory bodies and law enforcement agencies where disclosure is required by law.
- Information technology service providers and cloud hosting partners.
- Background screening, identity verification and right-to-work checking providers.
- Occupational health professionals and medical advisers where appropriate.
- Insurance providers and brokers.

- Banking and financial institutions for payment processing.
- Training providers and professional accreditation bodies.
- Other organisations where disclosure is required to fulfil contractual or legal obligations.

Personal information will only be shared to the extent necessary for the specific purpose concerned.

6.3 Safeguards When Sharing Data

Before disclosing personal information to any external organisation, the Company will take reasonable steps to ensure that:

- There is a valid legal basis for the disclosure.
- Only the minimum amount of personal information required is shared.
- Appropriate confidentiality obligations are in place.
- Suitable technical and organisational security measures are maintained by the recipient.
- The information will only be used for the agreed lawful purpose.
- The recipient complies with applicable data protection legislation.

Where third-party service providers process personal data on behalf of the Company, written agreements will be implemented to ensure that personal information is processed only in accordance with the Company's instructions and legal requirements.

6.4 International Transfers of Personal Data

As a general principle, Icon People Recruitment Ltd processes and stores personal information within the United Kingdom or other jurisdictions that provide an adequate level of protection for personal data.

Where it becomes necessary to transfer personal information outside the United Kingdom or to countries that do not benefit from an adequacy decision, the Company will ensure that appropriate safeguards are implemented before any transfer takes place.

Such safeguards may include:

- International Data Transfer Agreements (IDTAs).

- UK Addendum to the EU Standard Contractual Clauses.
- Other transfer mechanisms recognised under applicable data protection legislation.

These measures are designed to ensure that individuals' personal information continues to receive an equivalent level of protection.

6.5 Confidentiality

All employees, workers, contractors and any person acting on behalf of the Company are required to maintain the confidentiality of personal information obtained during the course of their duties.

Personal data must not be disclosed to unauthorised individuals, discussed in inappropriate settings, or accessed without a genuine business need.

Any unauthorised disclosure, misuse or negligent handling of personal information may result in disciplinary action and, where appropriate, legal or regulatory consequences.

6.6 Review of Data Sharing Arrangements

The Company will periodically review its data sharing practices and relationships with third-party organisations to ensure that they remain appropriate, secure and compliant with current legislation.

Where changes to legislation, business operations or contractual arrangements occur, data sharing procedures will be updated accordingly to maintain compliance with the UK GDPR, the Data Protection Act 2018 and other applicable legal requirements.

7. Responsibilities for Handling Personal Data

7.1 Responsibility for Data Protection

Protecting personal information is a shared responsibility across Icon People Recruitment Ltd. Every employee, worker, contractor, consultant, temporary worker, and any individual acting on behalf of the Company must ensure that personal data is handled securely, lawfully, and in accordance with this policy.

The Company has appointed a **GDPR Team** to oversee data protection compliance, provide guidance on privacy matters, monitor adherence to legal requirements, and support the continuous improvement of the Company's data protection framework.

Any questions relating to this policy or the handling of personal information should be directed to:

GDPR Team

Icon People Recruitment Ltd

11–15 Guildhall Lane

Leicester

LE1 5FQ

United Kingdom

Email: info@iconpeoplerecruitment.uk

7.2 Individual Responsibilities

Anyone processing personal data on behalf of the Company must ensure that they:

- Access personal information only when it is required to perform their authorised duties.
- Use personal data solely for legitimate business purposes.
- Process information fairly, lawfully and in accordance with Company policies.
- Keep personal information confidential at all times.
- Prevent unauthorised access, disclosure, alteration or misuse of personal data.
- Promptly report any suspected data protection concerns or security incidents.
- Complete any mandatory data protection or information security training provided by the Company.

Failure to comply with these responsibilities may expose both the individual and the Company to legal, financial and reputational risks.

7.3 Secure Handling of Personal Information

When processing personal data, all personnel must follow appropriate security practices, including:

- Ensuring documents containing personal information are stored securely.
- Locking computers or other devices whenever they are left unattended.
- Using strong passwords and keeping login credentials confidential.
- Preventing unauthorised individuals from viewing confidential information.
- Taking reasonable care when sending emails containing personal data.
- Verifying recipients before sharing confidential information.

- Avoiding discussions involving personal data in public or unsecured environments.
- Maintaining clear desk and clear screen practices wherever possible.

Only authorised personnel should have access to personal information necessary for their role.

7.4 Accuracy and Record Maintenance

Employees and authorised users must take reasonable steps to ensure that any personal information they create, update or manage is accurate, complete and kept up to date.

Where inaccurate or outdated information is identified, appropriate corrections should be made without unnecessary delay.

Individuals should also notify the Company promptly if their own personal details change so that Company records remain accurate.

7.5 Storage and Retention

Personal information should only be retained for as long as it is required for legitimate business purposes or to satisfy legal and regulatory obligations.

Employees must not retain duplicate, unnecessary or outdated records.

Once information is no longer required, it must be securely destroyed or permanently deleted in accordance with the Company's Data Retention Policy.

7.6 Use of Company Equipment

Personal information should only be accessed, processed or stored using authorised Company systems, equipment and approved software unless specific approval has been granted.

Employees must not:

- Store Company personal data on personal computers or personal mobile devices without authorisation.
- Transfer confidential information using unauthorised applications or cloud storage services.

- Download or copy personal data unless it is necessary for authorised business purposes.
- Leave electronic devices containing personal information unattended in public places or unsecured vehicles.

Where portable devices such as laptops or removable storage media are used, appropriate security measures, including password protection and encryption where available, must be applied.

7.7 Physical Security

Paper records containing personal information must receive the same level of protection as electronic records.

To safeguard physical information, employees should:

- Store confidential files in locked cabinets or secure storage areas.
 - Avoid leaving personal information unattended on desks, printers or meeting rooms.
 - Dispose of confidential documents using approved confidential waste or secure shredding facilities.
 - Ensure visitors and unauthorised persons cannot access confidential records.
-

7.8 Compliance and Monitoring

The Company reserves the right to monitor compliance with this policy through audits, inspections, security reviews and other appropriate measures.

Where weaknesses or areas for improvement are identified, corrective action may be implemented to strengthen data protection practices.

Deliberate misuse of personal information, unauthorised disclosure, negligence, or failure to comply with this policy may result in disciplinary action, which could include dismissal, termination of engagement, legal proceedings or regulatory action where appropriate.

Any intentional destruction, concealment or alteration of personal information relating to a lawful data access request or legal investigation may constitute a criminal offence under applicable legislation.

8. Personal Data Breaches

8.1 Commitment to Preventing Data Breaches

Icon People Recruitment Ltd is committed to protecting personal information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

The Company has implemented appropriate technical, organisational and administrative controls to reduce the likelihood of personal data breaches. Despite these measures, no system can guarantee absolute security. Therefore, all personnel have a responsibility to remain vigilant and to report any actual or suspected data breach immediately.

8.2 What is a Personal Data Breach?

A personal data breach is any security incident that results in the accidental or unlawful compromise of personal information.

Examples include, but are not limited to:

- Loss or theft of documents containing personal data.
- Misplacing laptops, mobile devices or storage media containing Company information.
- Sending personal information to the wrong recipient.
- Unauthorised access to Company systems or confidential records.
- Disclosure of personal information to individuals without proper authority.
- Cyber security incidents such as phishing attacks, malware, ransomware or hacking.
- Accidental deletion, corruption or alteration of personal data.
- Loss of availability of personal information where it affects individuals' rights.

Not every security incident will amount to a reportable personal data breach; however, every suspected incident must be assessed appropriately.

8.3 Reporting a Data Breach

Any employee, worker, contractor or person acting on behalf of the Company who becomes aware of an actual or suspected personal data breach must report it **immediately** to the Company's GDPR Team.

Reports should include, where possible:

- A description of what happened.
- The date and time the incident occurred or was discovered.
- The type of personal information involved.
- The number of individuals potentially affected.
- Any immediate actions already taken to contain the incident.
- Any other relevant information that may assist the investigation.

Prompt reporting enables the Company to minimise risks and comply with its legal obligations.

8.4 Investigation and Containment

Upon receiving notification of a suspected breach, the Company will take appropriate steps to:

- Assess the nature and severity of the incident.
- Contain the breach to prevent further loss or disclosure.
- Recover compromised information where possible.
- Identify the cause of the incident.
- Evaluate the potential impact on affected individuals.
- Implement corrective actions to reduce the risk of recurrence.
- Maintain appropriate records of the investigation and its outcome.

Every reported incident will be reviewed objectively and proportionately.

8.5 Notification Requirements

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Company will notify the **Information Commissioner's Office (ICO)** without undue delay and, where required by law, within **72 hours** of becoming aware of the breach.

If the breach is likely to result in a **high risk** to the affected individuals, the Company will also notify those individuals as soon as reasonably practicable.

Such notifications will include appropriate information regarding:

- The nature of the breach.

- The categories of personal information involved.
 - The likely consequences.
 - The measures already taken or proposed to address the incident.
 - Contact details for obtaining further information.
-

8.6 Recording Personal Data Breaches

The Company will maintain an internal record of all personal data breaches, regardless of whether they are reportable to the Information Commissioner's Office.

The breach register may include:

- Details of the incident.
- Date and time of occurrence.
- Categories of data involved.
- Number of individuals affected.
- Risk assessment findings.
- Corrective actions implemented.
- Lessons learned and preventive measures adopted.

Maintaining accurate records helps demonstrate compliance with UK data protection legislation and supports continuous improvement.

8.7 Responsibilities of Employees

Every individual working for or on behalf of Icon People Recruitment Ltd plays an important role in protecting personal information.

Personnel are expected to:

- Remain alert to potential security risks.
- Follow all Company data protection and information security procedures.
- Report suspected breaches immediately.
- Cooperate fully with any internal investigation.
- Take reasonable steps to minimise any further risk where it is safe and appropriate to do so.

- Participate in training and awareness programmes relating to data protection and cyber security.

Failure to report a known personal data breach or deliberate misuse of personal information may result in disciplinary action and, where appropriate, legal or regulatory consequences.

8.8 Continuous Improvement

Following every personal data breach or significant security incident, the Company will review its policies, procedures, systems and security controls to identify opportunities for improvement.

Where necessary, additional safeguards, employee training or technical measures will be introduced to strengthen data protection and reduce the likelihood of similar incidents occurring in the future.

9. Subject Access Requests (SARs)

9.1 Right of Access

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, individuals have the right to request confirmation of whether Icon People Recruitment Ltd is processing their personal data. Where this is the case, they may also request access to the personal information held about them, together with certain supplementary information regarding how that information is processed.

These requests are commonly referred to as **Subject Access Requests (SARs)**.

The Company is committed to responding to all valid requests in a transparent, timely and lawful manner.

9.2 Making a Subject Access Request

A Subject Access Request should normally be submitted in writing to enable the Company to accurately identify the information being requested.

Requests should be addressed to:

GDPR Team

Icon People Recruitment Ltd
11–15 Guildhall Lane
Leicester
LE1 5FQ
United Kingdom

Email: info@iconpeoplerecruitment.uk

Although no specific application form is required, individuals are encouraged to provide sufficient information to help the Company identify the relevant records and locate the requested information efficiently.

9.3 Verification of Identity

Before releasing any personal information, the Company may request reasonable evidence to verify the identity of the person making the request.

This safeguard helps ensure that personal data is disclosed only to the individual concerned or to someone who is legally authorised to act on their behalf.

Where additional identification is required, the response period will begin once satisfactory verification has been received.

9.4 Responding to Requests

The Company will acknowledge and assess each Subject Access Request without unnecessary delay.

Where the request is valid, a response will normally be provided **within one calendar month** from the date the request is received or, where applicable, from the date identity verification has been completed.

If a request is particularly complex or if multiple requests are submitted by the same individual, the Company may extend the response period by up to **two additional months**, as permitted under applicable legislation.

Where an extension is necessary, the individual will be informed of the reasons for the delay within the initial one-month period.

9.5 Information Provided

When responding to a Subject Access Request, the Company may provide:

- Confirmation of whether personal data is being processed.
- A copy of the personal information held.
- The purposes for which the information is processed.
- The categories of personal data involved.

- Details of recipients or categories of recipients with whom the information has been shared.
- The expected retention period or the criteria used to determine it.
- Information about the individual's rights under data protection legislation.
- Details of the source of the information where it was not obtained directly from the individual.
- Information regarding any automated decision-making or profiling, where applicable.

Certain information may be withheld where an exemption applies under the UK GDPR or the Data Protection Act 2018.

9.6 Fees

In most circumstances, Subject Access Requests will be processed **free of charge**.

However, where a request is clearly unfounded, excessive or repetitive, the Company reserves the right to:

- Charge a reasonable administrative fee to cover the cost of responding; or
- Refuse to comply with the request where permitted by law.

Any decision to charge a fee or refuse a request will be supported by appropriate legal justification.

9.7 Responsibilities of Employees

Any employee, worker or representative of the Company who receives a Subject Access Request must immediately forward it to the **GDPR Team** without attempting to respond independently.

Prompt escalation is essential to ensure statutory deadlines are met and that requests are handled consistently and in accordance with legal requirements.

Employees must never alter, delete, conceal or destroy personal information after becoming aware of a Subject Access Request.

Any deliberate interference with records that are subject to a lawful request may result in disciplinary action and could constitute a criminal offence under applicable legislation.

9.8 Record Keeping

The Company will maintain appropriate records of Subject Access Requests received, including:

- The date the request was received.
- Identity verification where applicable.
- Actions taken to process the request.
- Copies of the information provided.
- Any exemptions applied.
- Correspondence with the requester.
- The date the request was completed.

Maintaining accurate records enables the Company to demonstrate compliance with the UK GDPR, the Data Protection Act 2018, and its wider accountability obligations.

10. Rights of Data Subjects

10.1 Our Commitment

Icon People Recruitment Ltd is committed to respecting and protecting the rights of individuals whose personal information we collect and process. In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, every individual is entitled to exercise certain rights regarding their personal data.

The Company will respond to requests relating to these rights fairly, transparently and within the timescales required by law.

10.2 Right to be Informed

Individuals have the right to know how and why their personal information is collected, used, stored, retained and shared.

To ensure transparency, the Company provides information through this Data Protection Policy, its Privacy Notice and any other relevant privacy information issued at the time personal data is collected.

10.3 Right of Access

Individuals may request confirmation of whether the Company processes their personal data and, where applicable, request access to that information through a Subject Access Request (SAR).

The Company will respond to such requests in accordance with Section 9 of this policy and applicable data protection legislation.

10.4 Right to Rectification

Where personal information is inaccurate, incomplete or out of date, individuals have the right to request that it is corrected without unnecessary delay.

The Company will take reasonable steps to verify the accuracy of the requested amendment before updating its records.

10.5 Right to Erasure

Individuals may request the deletion of their personal information where one or more of the following applies:

- The information is no longer required for the purpose for which it was collected.
- The individual has successfully objected to the processing.
- Consent has been withdrawn and no other lawful basis exists.
- The personal data has been processed unlawfully.
- Erasure is required to comply with a legal obligation.

This right is not absolute. The Company may retain information where continued processing is required by law or is necessary to establish, exercise or defend legal claims.

10.6 Right to Restrict Processing

Individuals may request that the Company temporarily restrict the processing of their personal information in certain circumstances, including where:

- The accuracy of the information is being disputed.
- The processing is believed to be unlawful.
- The Company no longer requires the information but the individual needs it for legal purposes.

- An objection to processing is being considered.

While processing is restricted, the Company will continue to store the information but will only process it where permitted by law.

10.7 Right to Object

Where personal information is processed on the basis of the Company's legitimate interests or for direct marketing purposes, individuals have the right to object to such processing.

The Company will carefully assess every objection and will cease processing where required unless compelling lawful grounds exist that override the individual's rights and freedoms.

10.8 Right to Data Portability

Where processing is carried out by automated means and is based on consent or the performance of a contract, individuals may request a copy of their personal data in a structured, commonly used and machine-readable format.

Where technically feasible and legally permissible, the Company may transfer this information directly to another data controller upon request.

10.9 Rights Relating to Automated Decision-Making

Icon People Recruitment Ltd does not normally make decisions based solely on automated processing that produce legal or similarly significant effects on individuals.

Where automated decision-making or profiling is used in the future, it will only be undertaken where permitted by law and appropriate safeguards are in place. Individuals will be informed of such processing and of their rights in relation to those decisions.

10.10 Right to Withdraw Consent

Where the Company relies on an individual's consent as the lawful basis for processing personal information, that consent may be withdrawn at any time.

Withdrawal of consent will not affect the lawfulness of any processing carried out before the withdrawal was received.

Requests to withdraw consent should be submitted to the Company's GDPR Team.

10.11 Right to be Notified of a Personal Data Breach

Where a personal data breach is likely to result in a high risk to an individual's rights and freedoms, the Company will notify the affected individual without undue delay, unless an exemption applies under applicable legislation.

Such notifications will include appropriate information about the nature of the breach, the potential consequences and the measures taken to minimise its impact.

10.12 Right to Lodge a Complaint

If an individual believes that their personal information has been processed unlawfully or that their data protection rights have not been respected, they are encouraged to contact the Company's GDPR Team in the first instance so that the matter can be investigated and resolved promptly.

Individuals also have the right to submit a complaint directly to the **Information Commissioner's Office (ICO)**, the UK's independent supervisory authority for data protection matters.

Further information can be obtained from the ICO through its official website:
<https://www.ico.org.uk>

10.13 Exercising Your Rights

Requests relating to any of the rights described in this policy should be submitted to:

GDPR Team

Icon People Recruitment Ltd
11–15 Guildhall Lane
Leicester
LE1 5FQ
United Kingdom

Email: info@iconpeoplerecruitment.uk

The Company may request reasonable proof of identity before responding to any request to protect personal information from unauthorised disclosure.

Where a request cannot be fulfilled, either in whole or in part, the Company will explain the reasons for its decision and advise the individual of any available rights of review or complaint under applicable data protection legislation.