bluesource

Human Resources Privacy Policy

(HR)

Last updated 27th April 2026

At Bluesource, we are committed to protecting and respecting your privacy.

Your privacy is important to us. This Privacy Policy ("Policy") explains what personal data we collect, why we collect it, how it is used, the circumstances in which it may be shared, and the measures we take to keep it secure.

This Policy applies to individuals who are applying for employment or engagement with the Company, as well as to employees and workers. We may update this Policy from time to time, so you should review the latest version, which is available from the the HR Policy section the Company's Intranet and within the Employee Handbook, to ensure you remain informed of any changes.

Any questions regarding this Policy or our privacy practices should be directed to privacy@bluesource.co.uk or raised with the Head of Operations. If your query relates specifically to an HR matter, please contact human.resources@bluesoure.co.uk.

Who are we?

Bluesource Information Limited (the "Company") is private limited company registered in England, under number 4064193, with our registered office at: 122 Tooley Street, London, SE1 2TU. The Company comprises Bluesource Information Limited and its trading subsidiaries.

For the purposes of employment, engagement and related human resources activities, the Company acts as a Data Controller in respect of personal data relating to employees, prospective employees, and workers, and is registered with the Information Commissioner's Office under registration number ZA155583.

Legal basis for processing PII

To consider your application and, where appropriate, to offer you employment (or engagement) and enter into and perform an employment contract or other working arrangement with you, it is necessary for the Company to record, keep and process certain personal data about you, in electronic and hard copy form. Where reasonably necessary for these purposes and for the Company's responsibilities as an employer, this personal data may be shared with relevant parties, including other employees of the Company or any Group Company, the Company's professional advisers, payroll and benefits providers, HMRC, law enforcement, and regulators or other competent authorities. Where personal data is transferred outside the UK, appropriate safeguards will be applied. This processing does not affect your rights under the Data Protection Act 2018 and the UK GDPR.

How do we collect information from you?

Information you give us

If you apply for employment or engagement with the Company, or work with us as an employee or worker, you may be asked to provide certain personal information that is reasonably required to consider your application, enter into a contract or working arrangement, and manage the ongoing relationship. This includes information needed to meet legal and regulatory obligations, such as identity verification, right-to-work checks, taxation requirements and modern slavery legislation.

Personal information may be collected directly from you or provided by you through application forms, contracts, onboarding documentation, emails or other written communications.

Where you are engaged by the Company, we will also obtain and generate personal information during your employment or engagement, including where you take on specific responsibilities or roles, or participate in Company benefits or initiatives.

In addition, and in common with external contacts, personal information may be collected when you interact with our public websites, subscribe to Company updates, or engage with us via professional networking platforms.

We may also receive personal information from third parties, such as recruitment agencies, background screening providers or former employers, in connection with your application or engagement. Where this occurs, we expect such parties to have obtained the information lawfully and to have provided any required notices to you.

We may combine information you provide to us with information received from other sources where this is necessary and lawful.

Certain categories of personal data, including special category data (such as health-related records, credit check and criminal record check data), are collected only where strictly necessary, lawful, and subject to appropriate safeguards, and where required, an additional lawful basis under UK GDPR applies.

Information we get from the use of our services

In addition to the above, personal information may be included within documents and correspondence created or received during your application, employment or engagement, such as project documentation, proposals, contracts or other business records in which you are named or involved ("Documents").

Where you access or use Company systems, applications or services, we collect limited technical and usage information that is necessary for system operation, security, compliance and contractual performance. This may include:

- Details of access dates and times;
- Telephony and communication metadata (such as call duration and routing information);
- IP addresses used to access Company systems; and
- Information collected through cookies or similar technologies.

Further information on the use of cookies is set out in the Company's Cookie Policy, available at https://bluesource.co.uk/privacy-and-governance.

What type of information do we collect about you?

We collect and process personal data that is relevant, limited and necessary for the purposes of recruitment, entering into and performing an employment or engagement contract, managing the working relationship, and complying with our legal obligations as an employer.

The personal data we collect will vary depending on whether you are a prospective employee, employee or worker, and on the nature of the role. The categories of personal data typically collected, and the reasons for doing so, include the following.

Identity and contact information

- **Name** – to verify identity and uniquely identify you.
- **Date of birth** – to verify identity and, where applicable, administer pensions and statutory or insured benefits.
- **Personal contact details** – to communicate with you during recruitment and throughout the working relationship, and to administer HR processes and benefits.

- **Address and address history** – to verify identity, carry out pre-employment screening where required, and maintain accurate records.

Right to work and identity documentation

- **Passport, visa, driving licence and proof of address** – certified copies are obtained where necessary to verify identity, confirm right to work in the UK, meet regulatory requirements, or support work-related travel.
- **National Insurance number** – for payroll, taxation and statutory reporting purposes.
- **Bank details** – to enable payment of salary or fees and, where applicable, validate identity as part of pre-employment checks.

Pre-employment and ongoing screening

- **DBS checks** – A Disclosure and Barring Service (DBS) check is carried out for all prospective employees and workers as part of our recruitment and onboarding process. This is necessary to take steps prior to entering into an employment or engagement contract, to meet our contractual and regulatory obligations, and to support the Company's information security and safeguarding requirements.

  We retain only the minimum information required to evidence completion of the check, namely the certificate number, date of check and outcome. Full DBS certificates are not retained on the individual's HR file. Where a certificate is received by the Company, it is returned to the individual as their property.

  DBS information is processed with appropriate safeguards and in accordance with applicable data protection law.
- **Credit, fraud and sanctions checks** – undertaken as part of our recruitment and onboarding process, and may be repeated where required during employment. These checks are necessary to take steps prior to entering into an employment contract, to perform the employment contract, and to meet contractual, regulatory and information-security obligations.
- Credit checks are carried out only where lawful and proportionate, and, where required by law, with appropriate notice or consent. We retain only the minimum information necessary to confirm that the relevant checks have been completed, including a check reference, date and outcome, and process this information with appropriate safeguards.
- **Security Check clearance information** – where access to certain environments, systems or client work requires "Security Check" level clearance. Where a role involves access to client environments, systems or information that require security clearance (for example, "Security Check" or equivalent), we may process information relating to the existence, level, status and validity of that clearance where this is necessary to take steps prior to entering into a contract, to perform an employment or engagement contract, or to meet contractual or regulatory obligations.

  Prospective employees and workers who already hold relevant security clearance are required to seek transfer to Bluesource and their sponsors, where permitted by the issuing authority. Individuals must not allow an existing clearance to lapse or be terminated by their current employer or sponsor prior to confirming that a transfer or alternative sponsorship arrangement is in place, as this may affect our ability to offer or maintain employment or engagement.

  We do not retain full clearance certificates where this is not necessary. Information held is limited to what is required to confirm clearance status, validity and eligibility, and is processed with appropriate safeguards.

Recruitment and qualification information

- **Curriculum vitae, references and qualifications** – to assess suitability for a role and verify skills, experience and professional credentials.
- **Training and certification records** – where necessary to demonstrate competence, regulatory compliance or completion of training.

Emergency and benefits related information

- **Next of kin and beneficiary details** – held to enable contact in emergencies and to administer benefits such as pensions, death-in-service cover or insurance.
- **Partner and dependant details** – processed only where required to provide benefits that may extend to family members. Where information relates to children, it is provided by the individual with parental responsibility.

Special category personal data

We process special category personal data only where strictly necessary, lawful, and subject to additional safeguards. This includes:

- **Sickness and absence records** – to manage statutory and contractual sick leave, occupational health obligations and workforce planning.
- **Medical information** – obtained only where required for a specific purpose (for example, health and safety, reasonable adjustments or statutory requirements) and processed in accordance with UK GDPR Article 9.

Absence data may be analysed on an aggregated or statistical basis (for example, for attendance monitoring). Decisions affecting individuals are not based solely on automated processing, except where necessary for contractual performance.

Technical and system-related information

- **User and payroll identifiers, login credentials and access records** – to administer payroll, authenticate access to Company systems, ensure information security and maintain audit trails.
- **Role, department and work contact details** – to manage responsibilities, access rights, communications and organisational structure.
- **IP addresses and system usage data** – logged for security, compliance and operational purposes.
- **Cookies** – where you access Company websites, in accordance with our Cookie Policy.

Monitoring, CCTV and use of Company systems

The Company monitors the use of its premises, systems and services where this is necessary and proportionate for the purposes of security, crime prevention, health and safety, information security, regulatory compliance, and the performance and protection of employment or engagement contracts.

Such monitoring of premises, systems, communications or usage is carried out fairly, lawfully and transparently, and only where the Company has identified a clear and legitimate purpose, such as related to its information security policies and ISO 27001-certified information security management system. Monitoring is not carried out intrusively and is designed to be proportionate to the risks being managed.

Monitoring data is accessed strictly on a need-to-know basis, used only for the purposes for which it was collected, and retained for no longer than necessary. Individuals are not subject to decisions based solely on automated monitoring without appropriate safeguards.

Further information on specific monitoring activities, acceptable use of systems and individual responsibilities is set out in the Company's Information Security, Acceptable Use and related workplace policies.

CCTV

Closed-circuit television (CCTV) may be operated at Company premises for the purposes of safety, security and crime prevention. CCTV footage may capture images of employees, workers, visitors and other individuals. Access to CCTV footage is restricted to authorised personnel and recordings are retained only for as long as reasonably necessary, unless required for the investigation of an incident or to comply with a legal obligation.

Monitoring of access and system use

The Company monitors access to and use of its IT systems, networks, applications and physical facilities. This may include monitoring of:

- user log-ins and log-outs;
- access to systems, files and data;
- use of Company credentials;
- system usage, audit and security logs; and
- activity necessary to detect unauthorised access, misuse, security incidents or policy breaches.

Work communications and emails

Emails and electronic communications sent or received using Company-provided systems (including email, messaging and collaboration tools) may be monitored or accessed where necessary for security, legal, regulatory, operational or compliance purposes, or to investigate suspected misconduct or system misuse.

The Company does not routinely read personal communications. However, limited personal use of Company systems may incidentally result in the capture or processing of personal data. Individuals should therefore have no expectation of absolute privacy when using Company-owned systems or devices.

Personal use of Company systems

Limited personal use of Company IT systems is permitted in accordance with Company policy (such as defined in its Acceptable Use Policy). Where personal use occurs, personal data may be captured within system logs, communications or audit records. Individuals are encouraged to minimise personal use and avoid processing sensitive personal information using Company systems where possible.

Data minimisation and exclusions

We will not collect or retain personal data that is unnecessary for the purposes described above. We do not routinely process special categories of personal data such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, or data concerning sex life or sexual orientation, unless required by law or for equality monitoring purposes.

How we use the information about you?

We use personal data relating to prospective employees, employees and workers only where it is necessary, lawful and proportionate, and for the purposes set out in this Policy.

Personal data is processed to enable us to:

- **Take steps prior to entering into an employment or engagement contract**, including assessing suitability for a role and completing required pre-employment checks;
- **Enter into, administer and perform an employment or engagement contract**, including paying salary or fees and administering pensions, benefits and other contractual entitlements;
- **Provide benefits and services** associated with employment or engagement;
- **Meet information security requirements**, including protecting systems, data and assets, and meeting customer or contractual security obligations;
- **Identify and authenticate individuals** who are requesting access to systems, information or services;
- **Prevent and detect fraud, misuse, unauthorised access and security incidents**;
- **Manage workplace matters**, including investigating concerns, resolving disputes, enforcing policies and managing disciplinary or grievance processes;
- **Communicate with you** in relation to recruitment, your employment or engagement, and work-related matters;
- **Maintain business records**, where you are named as a contact or contributor in documents created or used in the course of business activities;
- **Analyse and improve internal processes and services**, including the use of aggregated or anonymised analytics where appropriate;
- **Gather feedback** to improve workplace practices, systems and services;
- **Monitor sickness and absence information** on a statistical or aggregated basis for workforce planning and compliance purposes;
- **Comply with legal, regulatory and statutory obligations**, including employment, tax, health and safety, equality and data protection requirements; and
- **Use automated or AI-enabled tools**, where applicable, to support operational processes in accordance with applicable law and internal governance policies.

Where personal data is processed for a new purpose that is not compatible with the purposes set out above, this will be assessed in advance and, where required by law, additional information will be provided.

Data location and international transfers

As a global company, we may process PII on our systems and servers around the world. We may process your personal information on a server located outside the country where you live, however we endeavour to store and host such systems and servers within the United Kingdom and the European Economic Area (“EEA”).

Where personal data is transferred outside the UK or EEA, appropriate safeguards are implemented in accordance with our Data Processing Policy (https://bluesource.co.uk/privacy-and-governance/data-privacy-and-processing), including adequacy regulations, transfer risk assessments, transfer impact assessments, UK International Data Transfer Agreements, or approved contractual safeguards, such as the implementation of standard contractual clauses.

Data retention

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected, including service delivery, regulatory compliance, dispute resolution, and enforcement of agreements.

Retention periods are defined by contractual, legal, regulatory, and operational requirements and are documented within the Company's internal Data Retention Policy. Data is securely deleted, anonymised or returned when no longer required, although some limited data may need to be indefinitely retained for compliance, legal and integrity purposes, such as contractual records, access logs and financial documents.

Transparency

We aim to be clear about what information we collect and why, so that individuals can make informed choices. We do not collect or retain personal data that is unnecessary for the stated purposes.

.

Your rights under UK GDPR

Under the UK General Data Protection Regulation (UK GDPR), you have a number of rights in relation to the personal information we hold about you. These rights apply to prospective employees, employees and workers, subject to certain legal conditions and limitations.

Your rights include:

- **The right to be informed**
  To be informed whether and how your personal data is being processed, including the purposes of processing, the legal basis relied upon, who the data is shared with, and how long it will be retained. This Privacy Policy is intended to provide key information about our HR-related data processing.
- **The right of access**
  To request access to the personal data we hold about you, and to receive a copy of that data, together with information about how and why it is processed.
- **The right to rectification**
  To request correction of inaccurate or incomplete personal data we hold about you.
- **The right to erasure (the "right to be forgotten")**
  To request deletion of your personal data where, for example:
  - it is no longer necessary for the purposes for which it was collected;
  - processing is based on consent and that consent has been withdrawn;
  - you have objected to processing and there are no overriding legitimate grounds; or
  - the data has been processed unlawfully or must be erased to comply with a legal obligation. This right is not absolute and may be limited where we are required to retain data by law.
- **The right to restrict processing**
  To request that processing of your personal data is restricted in certain circumstances, such as where you contest its accuracy or object to its use.
- **The right to data portability**
  Where applicable, to receive certain personal data you have provided to us in a structured, commonly used and machine-readable format, and to request that it be transferred to another controller.
- **The right to object**
  To object to the processing of your personal data where we are relying on legitimate interests or where processing is carried out for direct marketing purposes.
- **The right not to be subject to automated decision-making**
  To not be subject to decisions based solely on automated processing that produce legal or similarly significant effects, except where permitted by law and subject to appropriate safeguards.

Where you exercise your rights, we may request verification of your identity before responding. Some rights may be limited where exemptions apply or where exercising a right would adversely affect the rights of others.

For further information about your rights, please refer to the UK General Data Protection Regulation and guidance published by the Information Commissioner's Office.

Accessing and updating your personal information

The Company does not currently provide a self-service portal for personal data access. Requests to access, update, or delete personal data should be sent to privacy@bluesource.co.uk. We may require identity verification before acting on a request.

Requests may be declined where they are manifestly unfounded, excessive, technically impractical, or where legal retention obligations apply.

Automated decision-making

The Company does not carry out automated decision-making or profiling that produces legal or similarly significant effects for individuals.

Information that we share

We do not sell or rent personal data. We share personal data relating to prospective employees, employees and workers only where it is necessary, lawful and proportionate, and for the purposes set out in this Policy.

Contractual and work-related disclosures

Personal data may be shared where this is necessary to take steps prior to entering an employment or engagement contract, to enter into or perform such a contract, or to administer employment-related benefits and services (for example, payroll, pensions or insurance arrangements).

In these circumstances, we do not rely on “freely given consent”, as this is generally not appropriate in an employment context. Instead, processing is carried out on the basis of contractual necessity and legal obligation.

External processing and service providers

We may share limited personal data with trusted third parties who process information on our behalf, or jointly with us, under appropriate contractual and confidentiality arrangements. This includes third-party service providers supporting recruitment, background screening, HR administration, payroll, benefits administration and IT systems.

Such parties are permitted to process personal data only for the specific purposes instructed and are not authorised to use or disclose it for their own purposes. We share only the minimum personal data required for the relevant service.

Where communications are sent about optional products or services, this will occur only where any required consents have been obtained in accordance with applicable law.

Legal and regulatory disclosures

We may disclose personal data to external organisations or authorities where we believe in good faith that such disclosure is reasonably necessary to:

- comply with a legal obligation, court order, regulatory requirement or lawful request;
- establish, exercise or defend legal claims;
- investigate or prevent fraud, security incidents or other unlawful activity;
- protect the rights, property or safety of individuals, organisations or the public; or
- meet our obligations under data protection law, including breach reporting to the Information Commissioner’s Office.

Access controls and safeguarding

Access to personal data is restricted to employees, contractors and service providers who have a legitimate need to know in order to perform their role. Access rights are limited to the minimum necessary and subject to appropriate technical and organisational controls.

If we are involved in a merger, acquisition or asset sale, personal data may be transferred as part of that transaction. Where this occurs, we will ensure appropriate confidentiality protections and provide notice where required by law.

Whenever personal data is shared, we take reasonable steps to ensure it is handled securely and in accordance with this Policy and applicable data protection law.

Categories of third parties used for HR purposes

For HR-related purposes, personal data may be obtained, shared or processed by third parties under contractual arrangements to deliver specific services. These include, but are not limited to:

- recruitment agencies;
- pre-employment and ongoing screening providers;
- HR consultancy and advisory services;
- payroll, accounting and auditing providers;
- government and regulatory bodies (such as HMRC);
- HR and expense management systems;
- employee benefit and pension providers.

Permitted external data processors

As set out in the preceding section “Categories of third parties used for HR purposes”, the Company uses a range of external organisations to support recruitment, employment, engagement and related HR activities.

At any given time, the Company may use some or all of the external data processors listed below to process personal data on its behalf for HR-related purposes. These arrangements are subject to change as service providers are reviewed, replaced or updated.

All external data processors are engaged under appropriate contractual, confidentiality and data protection agreements, which require them to process personal data only on documented instructions from the Company, to apply suitable technical and organisational security measures, and to comply with applicable data protection law.

Personal data shared with external data processors is limited to the minimum necessary to deliver the relevant service.

The current permitted external service providers related to HR activities include:

Category of third party	Third Party	Purpose
Recruitment agencies	various	Applications and feedback on employment with relevant recruiters
Pre-employment screening	Due Diligence Checking and GOV.UK	Criminal record check from Disclosure Scotland which is an employment requirement for being able to offer employment
Pre-employment screening	HireRight	Criminal record check from Disclosure Scotland which is an employment requirement for being able to offer employment Credit and Sanctions check Fraud check
Pre-employment screening	Know Your Candidate	Credit and Sanctions check
HR consultancy	SME ADVISOR	External HR consultancy as an extension to in-house HR
HR consultancy	HR First	External HR consultancy as an extension to in-house HR
Financial	S&W Partners Group	Payroll and company auditors

Financial	HMRC	Taxes, etc.
HR related software as a service	E-days	Cloud based processing of employee leave, including holiday, sick leave and leave profiling
HR related software as a service	Concur	Employee expenses
Employee benefits	SLAIYBURN Financial Planning Ltd	MetLife intermediary
Employee benefits	MetLife	Death in Service insurance
Employee benefits	Workplace Pensions Direct ("WPD")	Pension intermediary and administration
Employee benefits	AVIVA	Company pension provision
Employee benefits (if applicable)	BUPA	Private Medical Insurance
Employee benefits (if applicable)	Others	Benefits offered to employees from time-to-time, such as salary sacrifice schemes for cycles, will require liaison with relevant providers, as applicable to the benefit.

Information Security

We protect personal data using appropriate technical and organisational measures designed to safeguard confidentiality, integrity, and availability against unauthorised access, alteration, disclosure, or destruction.

While no system can be guaranteed to be completely secure, the Company applies security controls proportionate to the risks identified and regularly reviews these measures to ensure they remain effective.

We operate an Information Security Management System ("ISMS") that is independently certified and maintained in accordance with recognised security standards, including ISO/IEC 27001, Cyber Essentials, and Cyber Essentials Plus.

If you have been given log-in details to provide you with access to certain services (for example software as a service type services), you are responsible for keeping those details confidential. This is also a requirement of the Company's Information Security policies and failure to abide by these is likely to result in a disciplinary matter.

Compliance and cooperation with regulatory authorities

We regularly review compliance with this Policy, UK GDPR, and the Data Protection Act 2018 as part of our ISMS.

Should I have a complaint, how do I report it?

To make it easy for our customers to raise a complaint, in the unlikely event they need to, we have a single email address that can be used complaints@bluesource.co.uk. We will determine whether the complaint is service, compliance or HR related and engage the necessary individuals to deal with the complaint for you.

If you remain dissatisfied, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk.

Changes

We may update this Policy and will notify customers of significant changes via direct notice or website publication.

Questions and Suggestions

If you have questions or suggestions, please complete a feedback form or you can contact us at: privacy@bluesource.co.uk.