1. Purpose and Scope

This Policy sets out mandatory data protection and information security requirements that apply to Suppliers (including subcontractors) who provide services to Bluesource Information Limited ("Bluesource") and/or Bluesource's customers. It applies to any access to Bluesource Systems and any handling of Bluesource Data in any form (electronic, paper, verbal).

Where this Policy is incorporated into an Agreement, compliance with this Policy is a material contractual requirement unless explicitly varied in writing. In the event of a conflict, the order of precedence is: (1) this Policy; (2) schedules/annexes to this Policy; (3) schedules to the Agreement; (4) the clauses of the Agreement.

2. Roles, Responsibilities and Contact Points

The Supplier must:

- Appoint a named information security and privacy contact / DPO (if applicable), who is responsible for compliance with this Policy and for incident coordination.
- Provide the current contact details (name, role, work address, work email, and work telephone number) to Bluesource on request and whenever they change.

All notifications should go to Bluesource's Information Security & Privacy Contact: Nick Jaggers, Head of Operations and DPO, +44 (0)20 7940 6200, nick.jaggers@bluesource.co.uk.

Privacy related queries may also be sent to Privacy@bluesource.co.uk and any complaints to ompliats@bluesource.co.uk.

3. Definitions

Key terms used in this Policy are defined in **ANNEX A - Definitions** and where a term is not defined here, it has the meaning given in the applicable Agreement and Data Protection Law.

4. Data Protection Obligations (Processor Requirements)

4.1 General

Where Supplier processes Bluesource Personal Data as a Data Processor (or Sub-Processor), Supplier shall comply with Data Protection Law and the instructions of Bluesource (or the relevant Bluesource customer acting as Controller, as applicable).

Supplier must not process Bluesource Personal Data for any purpose other than providing the Services as documented in **ANNEX B – Data Processing Summary / Instructions (Article 28) .**

Supplier must not combine or aggregate Bluesource Data with any third-party data unless approved in writing by Bluesource. The storage of Bluesource Personal Data shall be logically separated from all other third-party data unless such aggregation of data is authorised within the Services specification or, otherwise, by written agreement between the Parties.

4.2 Article 28 Processor Clauses (minimum requirements)

The Supplier must:

- Process Bluesource Personal Data only on documented instructions from Bluesource (including with regard to transfers).
- Ensure persons authorised to process Personal Data are subject to confidentiality obligations and receive appropriate training.
- Implement appropriate technical and organisational measures to protect Personal Data (see Section 5).
- Assist Bluesource with Data Subject requests and Controller obligations (e.g., DPIAs, consultations) to the extent relevant and technically feasible.
- Maintain records of processing activities as required for Processors and provide a summary to Bluesource on request.
- Delete or return Personal Data at the end of the Services in accordance with Section 4.6(Retention and Disposal), unless retention is required by law.
- Make available all information necessary to demonstrate compliance and allow audits as set out in this Policy, and in particular Section 4.5 and Section 5.14.

4.3 International Transfers

Supplier shall not transfer Bluesource Personal Data outside the UK and/or EEA without Bluesource's prior written approval. Where approved, Supplier shall implement an appropriate lawful transfer mechanism and supplementary measures where required. Supplier must disclose all processing and storage locations (including backup and disaster recovery locations) relevant to Bluesource Data.

4.4 Sub-processing

Supplier may only engage Sub-Processors with prior written authorisation from Bluesource and must maintain an up-to-date Sub-Processor register for the Services. Supplier shall flow down equivalent obligations to all Sub-Processors and remains fully liable for their acts and omissions.

The Supplier must:

- Provide Bluesource with at least 14 days' prior notice of any new or replacement Sub-Processor, including name, location(s), and services performed.
- Maintain evidence of due diligence and ongoing monitoring of Sub-Processors (including security assurance).
- Notify Bluesource of any material change in Sub-Processor risk profile or security posture without undue delay.

4.5 Audit and Assurance

Supplier shall provide reasonable assurance of compliance with this Policy. Bluesource (or its customers where applicable) may audit Supplier's compliance no more than once per calendar year unless required by a regulator or following a material incident. Where an audit identifies non-conformities, Supplier shall provide a remediation plan with agreed timelines and evidence of closure.

4.6 Data Minimisation, Retention, and Secure Disposal

The Supplier must:

- Minimise collection and access to Bluesource Personal Data to what is necessary for the Services.
- Maintain and apply a documented retention schedule for Bluesource Personal Data or define retention criteria in the Agreement.
- At termination or on request, securely return or delete Bluesource Data (including backups where practicable) and provide a deletion/destruction certificate.

- Where retention is required by law, provide written details of the data retained, legal basis, retention period, and protective controls.

4.7 Use of Live Data in Non-Production Environments

Supplier must not use live Bluesource Personal Data in development, test, staging, training, or demonstration environments without Bluesource's prior written consent and documented safeguards (e.g., anonymisation/pseudonymisation, restricted access, time-bounded retention).

4.8 Use of Bluesource Data in AI

Supplier must not, without the express written permission of Bluesource:

- Use Bluesource Data, including Bluesource Personal Data, as a source of data to model AI,
- Process Bluesource Data using AI,
- Automate a decision based on AI.

Section 5.13, relating to the security of AI, must always apply.

5. Information Security Requirements (Security Measures)

Supplier must:

5.1 Security Management and Governance

- Maintain an Information Security Management System (ISMS) aligned to ISO/IEC 27001 (or equivalent) appropriate to the Services and commensurate with the level of risk posed by its processing and the sensitivity of the Bluesource Data.
- Define security roles and responsibilities and maintain security policies and procedures covering the Services.
- Perform risk assessments for the Services at least annually and upon material change.
- Maintain an inventory of assets and data flows supporting the Services, including hosting and backup locations.
- Upon request, provide relevant evidence to support Supplier's security management and governance, such as copies of relevant certifications, data flows, risk assessments, policies.

5.2 Personnel Security

- Conduct pre-employment screening appropriate to role and data sensitivity (identity, right-to-work, references; and criminal record checks where lawful and proportionate).
- Provide security and data protection training on onboarding and at least annually thereafter.
- Ensure confidentiality obligations and disciplinary processes exist for policy breaches.

5.3 Access Control and Identity

- Apply least privilege and role-based access; no shared accounts should be used and privileged access should wherever possible use separate accounts to clearly identify admin type activity.
- Enforce Multi-Factor Authentication (MFA) for administrative accounts and for all remote access to environments processing Bluesource Data.
- Implement strong authentication: minimum 12-character passwords (or passphrases) and protect against reuse; rotate credentials when compromise is suspected or when personnel change roles.
- Review access rights at least quarterly and promptly remove access on role change or termination.
- Use device locking (max 5 minutes inactivity) and secure screen locking on all endpoints accessing Bluesource Data.

5.4 Cryptography and Key Management

- Encrypt Bluesource Data in transit using TLS 1.2 or above and at rest using strong industry-standard encryption (e.g., AES-256 or equivalent).
- Protect encryption keys using appropriate key management controls (segregation of duties, access logging, rotation, and secure storage).
- Do not weaken or disable security controls (e.g., TLS validation) without Bluesource's written approval.

5.5 Endpoint, Network and Malware Protection

- Maintain hardened, patched standard builds for servers and endpoints.
- Deploy reputable endpoint protection/EDR and maintain up-to-date malware signatures.
- Use firewalls and network security controls (IDS/IPS where appropriate) to protect environments processing Bluesource Data.
- Separate test, development, production and public networks, with adequate protection for access and traffic between the networks.

5.6 Vulnerability and Patch Management

- Operate vulnerability management covering infrastructure, applications and dependencies.
- Remediate Critical vulnerabilities within 14 days; High within 30 days (or implement compensating controls with documented risk acceptance agreed with Bluesource).
- Perform vulnerability scans at least monthly and after significant changes.
- Maintain a documented process for coordinated vulnerability disclosure and promptly notify Bluesource if a vulnerability may affect the Services and or Bluesource Data.

5.7 Secure Development (where Supplier develops or customises software)

- Follow a Secure Development Lifecycle (SSDLC) including code review and security testing.
- Use segregated dev/test and production environments.
- Do not use Bluesource Data for testing without consent (see Section 4.7).
- Maintain dependency management and remediate known vulnerable components promptly.

5.8 Logging, Monitoring and Detection

- Generate logs sufficient to attribute actions to individuals and to investigate security events.
- Protect logs from unauthorised alteration and retain security logs for at least 12 months (or longer if required by law/contract).
- Monitor for suspicious activity and investigate alerts in a timely manner.

5.9 Physical & Environmental Security

- Restrict physical access to areas housing systems processing Bluesource Data using appropriate controls (access controls, badging, visitor logs, CCTV where appropriate).
- Securely store and dispose of hard copy records and media using approved methods (e.g., cross-cut shredding, certified destruction).
- Protect systems processing Bluesource Data from environmental and physical risks, such as fire and flooding, using appropriate controls (fire alarms, smoke detectors, use of virtual infrastructure).

5.10 Cloud and Hosted Services (where applicable)

- Obtain Bluesource's written approval before using public cloud services or changing hosting/sub-hosting arrangements for the Services.
- Disclose data residency (primary, backup and DR regions) and ensure Bluesource Data is logically segregated from other customers.
- Only process Bluesource Data on systems hosted within the UK or EEA unless Bluesource's prior written consent has been give.
- Conduct independent penetration testing of internet-facing services at least annually and remediate findings in agreed timelines.
- Maintain a cloud security assurance framework (e.g., CSA CCM or equivalent) appropriate to the Services.

5.11 Business Continuity and Disaster Recovery

- Maintain and test business continuity and disaster recovery plans at least annually and ideally every 6 months.
- Define and provide service recovery targets (RTO/RPO) appropriate to the Service criticality and agreed with Bluesource.
- Ensure backups are encrypted, tested at least quarterly wherever possible, and protected from unauthorised access.

5.12 Incident Response and Notification

- Maintain an incident response process including triage, containment, eradication, recovery and post-incident review. Supplier must preserve evidence for forensic purposes where legally permissible.
- Wherever possible and no later than within 24 hour, notify Bluesource of any suspected or confirmed Information Security Incident affecting Bluesource Data or Systems within 1 hours of becoming aware (telephone + email), providing the minimal information detailed in **ANNEX B – Data Processing Summary / Instructions (Article 28).**
- Provide an initial written report within 12 hours wherever possible, and no later than 24 hours, and provide daily updates until resolution or as otherwise agreed.
- Do not notify Data Subjects, Data Processing Regulator, other regulators, or third-parties without Bluesource's written consent unless legally required; where legally required, notify Bluesource before disclosure (where lawful).
- Cooperate fully with Bluesource investigations and provide relevant logs and evidence promptly.
- Assist Bluesource and/or the relevant Data Controller as per its obligations under relevant Data Protection Law, as the Processor for the Service(s).

5.13 Use of AI / External Processing Tools

- Supplier must not input, upload, or otherwise disclose Bluesource Data into public or third-party AI/ML tools (including LLM assistants) without Bluesource's prior written approval.
- Where approved, Supplier must document the tool, data types, processing purpose, retention, and safeguards, and ensure no training of third-party models on Bluesource Data unless explicitly agreed in writing.

5.14 Compliance, Testing and Right to Audit

- Maintain relevant security certifications or independent assurance reports (e.g., ISO 27001 certificate, SOC 2 Type II, Cyber Essentials, Cyber Essentials Plus) and provide summaries to Bluesource on request.
- Perform independent penetration testing at least annually (for internet-facing systems) and provide an executive summary and remediation status on request.
- Allow Bluesource to perform reasonable assurance activities, including questionnaires, evidence requests, and audits, subject to confidentiality and reasonable notice.

5.15 Change management

- All IT system changes related to and providing the Services shall be reviewed, tested, and deployed using a formal change management process.
- Any planned downtime and periods of possible disruption to the services must be communicated in advance to Bluesource, at least 48 hours in advance.

5.16 Acceptable Use Policy

- Where Supplier personnel will have access to Bluesource Data and/or Bluesource Systems, including that of its Customer's, it must abide by Bluesource's and/or the relevant Customer's Acceptable Use Policies, which shall be made available to the Supplier on request.

5.17 PCI

- To the extent Supplier collects, stores, transfers, or processes any Payment Data, Supplier acknowledges and agrees that it is responsible for the security of such Payment Data and will comply and maintain compliance with the most current PCI Standards as well as this Security Policy. Upon Bluesource's reasonable request, Supplier will provide attestations of such compliance.

  For the purposes of this Policy, "**Payment Data**" means a credit or debit card holder's credit or debit card account number, bank account number, name, service code, security code, card validation code or value (e.g., CVV number), expiration date, magnetic stripe data, PIN, PIN block, and/or password, which is (a) disclosed or furnished, in any form, by Bluesource, its associates, agents or employees to Supplier in connection with Supplier's performance of the Services, or (b) collected, stored, processed, transmitted, accessed or used by Supplier in connection with Supplier's performance of the Services.

6. Survival

- The provisions of this Policy will survive the expiration or earlier termination of an Agreement and will only cease once Supplier ceases to process or hold any Bluesource Data.

7. ANNEX A - Definitions

"Agreement" means any written agreement, master service agreement, contract, sow, service schedule or other such document agreed between Bluesource and Supplier, together the Parties.

"Bluesource Data" means, collectively and individually, all data and information including, without limitation, confidential information and Personal Data which is (a) disclosed or furnished, in any form, by Bluesource, its customers, associates, agents or employees to Supplier in connection with Supplier's performance of the Services, or (b) collected, stored, processed, transmitted, accessed or used by Supplier in connection with Supplier's performance of the Services.

"Bluesource Personal Data" means Bluesource Data that is considered as Personal Data.

"Bluesource Systems" means collectively and individually, Bluesource's, its customers' and associates' information systems, applications, databases, infrastructure, platforms, and networks.

"Customer" means collectively and individually Bluesource, its customers and associates.

"Data Protection Law" means all applicable data protection and privacy legislation, regulations and guidance including Regulation (EU) 2016/679 (the "General Data Protection Regulation" or the "GDPR") and Data Protection Act 2018 ("DPA"), and all legislation enacted in the UK in respect of the protection of personal data) and the Privacy and Electronic Communications (EC

Directive) Regulations 2003 (all as amended, updated or re-enacted from time to time).

"Data Controller" has the meaning given to it in Data Protection Law.

"Data Processor" has the meaning given to it in Data Protection Law**.**

"Data Privacy Incident" means any: a) Disclosure of Personal Data by Supplier in violation of this Security Policy or applicable laws pertaining to data protection or data security, or b) Other unauthorised, accidental, or unlawful access, acquisition, disclosure or use of Personal Data that has occurred or may have occurred, including, without limitation, any unauthorised access of which Supplier is notified or suspects.

"Data Processing Regulator" means the Information Commissioner's Office and any other data protection supervisory authority with jurisdiction over either party and/or their Processing activities, and in each case any successor body from time to time.

"Data Subject" has the meaning given to it in Data Protection Law.

"Information Security Incident" means any: a) Data Privacy Incident, or b) any event, activity or occurrence that threatens or may threaten the confidentiality, integrity and/or availability of the Systems.

"Parties" shall refer to both Bluesource and the Supplier, as parties to a contractual arrangement.

"Personal Data" has the meaning given to it in Data Protection Law.

"Policy" means this **"**DATA PROTECTION & INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS" policy.

"Process", **"Processing"** and **"Processed"** each has the meaning given in Data Protection Law.

"Service" means the service/s provided to Bluesource, its customers, or associates.

"Supplier" means a supplier of services to Bluesource and/or Bluesource's customers.

"Supplier Systems" means Supplier's information systems, processes, facilities, applications, databases, infrastructure, platforms, and networks (a) utilised to provide the Services, (b) collecting, storing, processing, transmitting, accessing, or using Bluesource Data, and/or (c) with access to, connection to, use of or otherwise interacting with Bluesource Systems.

"Systems" means collectively Bluesource Data, Bluesource Systems and Supplier Systems.

8. ANNEX B – Data Processing Summary / Instructions (Article 28)

Unless otherwise agreed in writing by the Parties, the following Data Processing Instruction shall apply as a "Data Processing Summary", as required by Article 28 of GDPR:

DATA PROCESSING SUMMARY / INSTRUCTION FOR PROCESSING	
In respect of services, application and/or systems containing Bluesource Personal Data:	
	Response
Purpose for which the Personal Data shall be processed and its legal basis, and nature of consent.	The legal basis for processing PII related to providing Information Technology related services to Bluesource and/or its customers, and maintain a contractual relationship [GDPR, Article 6,1 (b)]. Without the appropriate Personal Data, the services and Agreement/s could not be maintained.

Nature of processing	Storing, accessing, and reviewing Personal Data in accordance with the terms of the Agreement and any applicable statement of work or services specification form.
Description of the categories of the Data Subjects	The Data Subjects, who's appropriate Personal Data may be processed during the provision of services under Agreement include: - Bluesource employees, subcontractors or associates; - Bluesource customer employees, associates, contractors and subcontractors; using a service provided by Supplier under Agreement; - Supplier employees necessary to procure and provide services to Bluesource.
Description of the categories of Personal Data	Personal Data includes but not limited to: - Names; - Job titles; - Departments; - Address; - Email addresses; - Telephone numbers. Certain Services, and access to websites and portals, may also capture necessary login details, cookies and IP addresses for authentication, security, and customisation purposes. Further details can be found in Supplier's privacy and cookie policies, which may be updated from time to time.
Categories of Special Category Data	Through the normal course of providing this type of services, Supplier would not normally process Special Categories of Personal Data, as defined by Data Protection Laws.
Description of transfers of Personal Data to a country outside of the EEA.	Supplier will not transfer or process Bluesource Personal Data outside of the EEA without the prior written authorisation of Bluesource.
Duration of Processing	Supplier will retain Personal Data for as long as necessary to deliver services under Agreement and relevant for their operations or to comply with relevant laws. In addition, Supplier may need to retain certain Personal Data after termination of the relationship to comply with laws or legislation, prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation, enforce our policies and agreements, and take other actions permitted or required by applicable laws.
General description of technical and organisational security measures	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the severity of the risks to the rights and freedoms of natural persons, take and maintain appropriate technical and organisational measures (including, where applicable, complying with Bluesource's policies and procedures relating to data protection) in relation to the Personal Data to ensure a level of security appropriate to the level of risk (and in assessing risk shall take account, in particular, of the risks that are presented by processing in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data). Such measures shall include inter alia as appropriate: - Access control on a "who needs to know, minimum rights" basis for both electronic and paper-based data, - Maintaining an information security management system to ISO27001, - Minimising the processing of Personal Data, - The pseudonymisation and encryption of Personal Data, - Transparency with regards to the functions and processing of Personal Data, - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and - A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;". These measures/controls may be updated from time to time.

Authorised Sub-Processors	The Supplier shall not engage subcontractors, except Authorised Subcontractors, without the prior written authorisation of Bluesource senior management.

The processing details for the Services must be completed per service/statement of work. The minimum fields include:

- Purpose, lawful basis, and nature of any consent relied upon (if applicable).
- Nature of processing (e.g., access, storage, support).
- Categories of Data Subjects.
- Categories of Personal Data and any Special Category Data.
- Transfers outside the UK/EEA (locations, mechanisms).
- Processing duration and retention criteria.
- Technical and organisational measures (TOMs) applied.
- Authorised Sub-Processors list.

9. ANNEX C – Incident Notifications

All incidents reported to Bluesource must include the following minimum content:

- Date/time discovered; date/time occurred (if known).
- Description of incident type and systems/data affected.
- Approximate number of records and Data Subjects affected (if known).
- Containment and remediation actions taken/planned.
- Indicators of compromise and forensic preservation steps.
- Point of contact and next update time.

10. SUMMARY

This policy document outlines the mandatory data protection and information security requirements for suppliers providing services to Bluesource Information Limited and its customers, covering all forms of data handling and system access.

- **Applicability and contractual precedence:** The policy applies to all suppliers and subcontractors handling Bluesource data and accessing its systems, with compliance being a material contractual obligation unless otherwise agreed in writing, and a defined order of precedence for conflicting terms.
- **Supplier responsibilities and contacts:** Suppliers must appoint designated security and privacy contacts responsible for compliance and incident management, providing their details to Bluesource, which also specifies its own contact points.
- **Data protection obligations for processors:** Suppliers processing personal data must comply with data protection laws and Bluesource's instructions, limiting processing to service provision purposes, and adhere to detailed processor requirements including confidentiality, training, technical measures, assistance with data subject requests, record keeping, data return or deletion, and audit cooperation.
- **International transfers and sub-processing:** Personal data transfers outside the UK/EEA require prior written approval and lawful mechanisms; sub-processors may only be engaged with Bluesource's authorization, must be registered, and suppliers remain liable for their compliance, including due diligence and timely notification of changes.
- **Audit, data minimization, retention, and secure disposal:** Suppliers must provide compliance assurance through audits, minimize data collection, maintain retention schedules, securely return or delete data at service end with certificates, and document lawful retention cases.
- **Restrictions on use of live data in non-production environments:** Live personal data cannot be used in development or testing environments without prior written consent and required safeguards such as anonymization and restricted access.

- **Information security requirements:** Suppliers must maintain an ISO/IEC 27001-aligned ISMS, perform risk assessments, enforce personnel security including screening and training, apply strict access controls with MFA, secure cryptographic measures, endpoint and network protections, vulnerability management, secure software development practices, comprehensive logging and monitoring, physical security, cloud service controls, business continuity planning, and incident response protocols with prompt notification and cooperation.
- **Use of AI and external processing tools:** Suppliers are prohibited from inputting Bluesource data into public or third-party AI/ML tools without prior approval, and must document and safeguard any approved use, explicitly forbidding training third-party models on such data unless agreed.
- **Change Control:** Supplier must have change control in place and provide at least 48 hours' notice of changes that affect or may affect the Service.
- **Payment Data:** To the extent Supplier collects, stores, transfers, or processes any Payment Data, Supplier acknowledges and agrees that it is responsible for the security of such Payment Data and will comply and maintain compliance with the most current PCI Standards as well as this Security Policy.
- **Acceptable Use:** Where Supplier personnel will have access to Bluesource Data and/or Bluesource Systems, including that of its Customer's, it must abide by Bluesource's and/or the relevant Customer's Acceptable Use Policies.
- **Compliance certifications and audit rights:** Suppliers must maintain relevant security certifications or assurance reports, conduct annual penetration testing for internet-facing systems, and allow Bluesource reasonable assurance activities including audits with confidentiality and notice provisions.

11. Policy Sign-Off

On behalf of Bluesource	
Name	Nick Jaggers
Position	Head of Operations
Signature	
Date	19th March 2026

12. Revision History

15/03/2023	Nick Jaggers	Policy created with ISO27002:2022 references.
11/03/2024	Nick Jaggers	Annual review and rebranding.
08/03/2025	Nick Jaggers	No changes required.
19/03/2026	Nick Jagers	Re-written after GAP analysis in line with changes in legislation for GDPR and EU data protection..