Bluesource

Supplier Code of Conduct

Last updated 8th May 2026

1 Overview

Bluesource Information Limited ("**Bluesource**") is committed to conducting its business ethically, lawfully, and with integrity, and to ensuring that these standards are upheld across its supply chain.

This Supplier Code of Conduct ("**SCoC**") establishes the minimum standards of ethical, legal, security, and sustainability practices expected of all suppliers, subcontractors, and third-party providers ("**Suppliers**") who deliver goods or services to, or on behalf of, Bluesource.

This Code forms part of Bluesource's Information Security Management System (ISMS) and wider governance and compliance framework, and supports the Company in meeting its legal, regulatory, contractual, and ethical obligations.

The SCoC is aligned with:

- The Bluesource Company Code of Conduct, which sets overarching standards of behaviour;
- The United Nations Global Compact (UNGC) Ten Principles, covering human rights, labour, environment, and anti-corruption; and
- Applicable laws, regulations, and recognised industry standards, including ISO/IEC 27001.

Suppliers are expected to operate in a manner consistent with these principles and to:

- Act professionally, ethically, and with integrity in all business dealings;
- Comply with applicable legal, regulatory, and contractual requirements;
- Protect Bluesource and customer information; and
- Promote responsible and sustainable business practices across their operations and supply chains.

Failure to meet these expectations may result in corrective action, enhanced monitoring, or termination of the supplier relationship, in accordance with contractual and governance requirements.

2 Purpose

The purpose of this Supplier Code of Conduct is to:

- Define clear expectations of professional, ethical, and lawful conduct for Suppliers;
- Support compliance with legal, regulatory, contractual, and information security obligations;
- Align Supplier behaviour with Bluesource's values, governance framework, and ethical standards;
- Reinforce commitment to responsible and sustainable business practices, including:
  - Respect for human rights;
  - Fair labour practices and non-discrimination;
  - Environmental responsibility; and
  - Zero tolerance for bribery, corruption, and unethical conduct;
- Establish a framework for supplier accountability, assurance, and continuous improvement, supporting effective supply chain risk management.

3 Scope and Applicability

This Code applies to all Suppliers who:

- Deliver goods or services directly to the Company;
- Process, store, or access the Company or its customers' information; or
- Act on behalf of the Company in any capacity.

Suppliers are responsible for ensuring that their personnel, subcontractors, and supply chain comply with this Code.

Where requirements overlap with other policies, the higher ethical, legal, or compliance standard shall apply.

4 Governance and Framework Alignment

This Code forms part of the Company's ISMS and should be read alongside:

- Company Code of Conduct;
- Data Protection and Information Security Requirements for Suppliers;
- Anti-Bribery and Corruption Policy;
- Sustainability Policy; and
- Other relevant contractual and regulatory requirements.

Copies of these Company policies are published on the Company's website at https://bluesource.co.uk/privacy-and-governance, and are subject to regular review and revisions, as necessary to reflect operational and regulatory changes.

5 Supplier Responsibilities

Suppliers must:

- Act lawfully, ethically, and with integrity;
- Comply with all applicable laws and contractual obligations;
- Maintain appropriate policies, procedures, and controls;
- Promptly report actual or suspected non-compliance;
- Cooperate with the Company on audits, investigations, and assurance activities; and
- Ensure equivalent standards are applied throughout their supply chain.

5.1 *Information Security and Data Protection*

Suppliers must:

- Comply with applicable data protection laws, including UK GDPR and, where applicable, EU GDPR;
- Comply with the Company's Data Protection and Information Security Requirements for Suppliers Policy in relation to the performance of services to the Company and its customers, except as otherwise agreed in writing between the Parties.
- Protect Company and customer information in accordance with contractual and policy requirements;

- Implement and maintain an appropriate information security management system proportionate to risk;
- Apply data classification, access controls, and least privilege principles;
- Conduct regular risk assessments for confidentiality, integrity, and availability;
- Ensure subcontractors are subject to equivalent obligations;
- Support security assurance activities, including audits and evidence requests;
- Provide appropriate training and awareness to personnel on an annual basis and test their understanding;
- Not further process Bluesource or Bluesource's customers data other than intended or for longer than reasonably necessary.
- Report security incidents or data breaches promptly in line with contractual obligations; and
- Maintain appropriate business continuity and disaster recovery capabilities.

If a Supplier is requested or required to disclose any Company and/or Company customer's confidential information under a subpoena, court order, statute, law, rule, regulation, regulatory request or other similar requirement (a "Legal Requirement"), the Supplier must, to the extent not precluded by law, provide prior prompt notice of such Legal Requirement to the Company prior to the disclosure.

5.2 *Business Ethics and Integrity (UNGC Principle 10)*

Suppliers must:

- Comply with all applicable laws relating to bribery, corruption, fraud, and money laundering;
- Disclose conflicts of interest promptly;
- Maintain accurate and complete business records;
- Provide accurate and truthful information;
- Avoid misleading statements or misrepresentation; and
- Conduct business in a manner that upholds the Company's reputation for integrity and professionalism.

5.3 *Gifts and Hospitality*

Suppliers must ensure that any gifts or hospitality:

- Are lawful, proportionate, and transparent;
- Are not intended to influence business decisions;
- Do not include cash or cash equivalents;
- Are not provided to public officials or political representatives; and
- Comply with applicable anti-corruption laws and policies.

5.4 *Human Rights (UNGC Principles 1–2)*

Suppliers must:

- Respect internationally recognised human rights;
- Prohibit child labour, forced labour, and human trafficking;
- Implement processes to identify and mitigate human rights risks;

- Provide safe and secure working environments; and
- Comply with applicable labour laws and standards.

Suppliers must avoid actions that cause, contribute to, or are directly linked to adverse human rights, environmental, or ethical impacts through their operations or business relationships.

5.5 *Labour, Inclusion and Diversity (UNGC Principles 3–6)*

Suppliers must:

- Prohibit discrimination in employment practices;
- Promote equality, diversity, and inclusion; and
- Ensure fair treatment for all personnel.

5.6 *Environmental Responsibility (UNGC Principles 7–9)*

Suppliers must:

- Actively support environmentally responsible practices aligned with the Company's Sustainability Policy;
- Manage and reduce environmental impacts;
- Consider lifecycle impacts of goods and services; and
- Provide sustainability information or metrics upon reasonable request, particularly where suppliers contribute to the Company's Scope 3 emissions.

5.7 *Health and Safety*

Suppliers must:

- Provide safe and healthy working environments;
- Comply with applicable health and safety laws; and
- Implement appropriate health and safety management systems.

5.8 *Professional Conduct in the Workplace*

Suppliers and their workers are expected to:

- Behave professionally and respectfully at all times;
- Communicate appropriately and constructively; and
- Adhere to Company behavioural standards.

Unacceptable conduct includes:

- Bullying, harassment, or discrimination;
- Misuse of Company systems or resources; and
- Breaches of confidentiality.

5.9 *Social Media and External Communications*

Suppliers must ensure that any public communications, including social media activity, do not:

- Misrepresent the Company or its services;
- Disclose confidential or sensitive information; or
- Damage the Company's reputation or relationships.

Where Suppliers individuals identify themselves as associated with the Company, they must ensure that their conduct is consistent with the standards set out in this Code.

5.10 *Use of Company and Company Customer Assets*

Company assets and those entrusted to it (including IT systems, data, and intellectual property) must:

- Be classified and handled appropriately in accordance with a suitable data classification and asset management policies, and retain any Company set classifications;
- Must be returned or destroyed after user, in accordance with the Company's instructions and its Data Protection and Information Security Requirements for Suppliers Policy;
- Be used only for legitimate business purposes;
- Be protected from unauthorised access, loss, or misuse;
- Not be removed or copied without authorisation;
- Not reused or reprocessed for any other purpose.

For more detailed information on the use of assets, please refer to he topic specific polices detailed above.

6 Monitoring, Assurance and Enforcement

The Company may require Suppliers to:

- Provide evidence of compliance;
- Participate in audits and assessments; and
- Support investigations into breaches.

Failure to comply may result in:

- Corrective action plans;
- Increased monitoring;
- Suspension or termination of the relationship; or
- Legal or contractual remedies where appropriate.

The Company will endeavor to work with its Suppliers to ensure they are compliant and where necessary, review any identified corrective action plans. Failure to meet these requirements may result in remediation plans, suspension, or termination of the supplier relationship.

7 Whistleblowing and Reporting

Suppliers must:

- Report concerns relating to legal, regulatory, or ethical misconduct, including:
  - accounting, internal accounting controls or auditing matters;
  - regulatory compliance;
  - bribery or other improper payments;
  - potential money laundering or other suspicious activity;
  - inappropriate conflicts of interest;
  - the integrity of Bluesource's accounting practices, internal controls, auditing matters or public filings; and
  - improper or questionable behavior by employees, supervisors, clients, counterparties, consultants, suppliers or other third parties.
- Support investigations; and
- Ensure that reporting mechanisms are available to their personnel.

The Company treats all reports confidentially and prohibits retaliation against individuals raising concerns in good faith.

8 Responsibilities

Bluesource Responsibilities

Bluesource is responsible for:

- Defining and maintaining this Supplier Code of Conduct and reviewing it at least annually.
- Making this Code available to Suppliers and communicating expectations clearly.
- Assessing supplier compliance where appropriate, including through proportionate due diligence, assurance activities, or reviews.
- Working with Suppliers in good faith to address identified issues and agree corrective actions where noncompliance is identified.
- Taking proportionate action where Suppliers fail to meet the requirements of this Code.

Supplier Responsibilities

Suppliers are responsible for:

- Complying with all requirements set out in this Supplier Code of Conduct.
- Ensuring that relevant personnel, subcontractors, and subprocessors understand and adhere to its requirements.
- Complete any required training and awareness activities relating to this Code;
- Maintaining appropriate policies, processes, and controls to meet legal, contractual, security, ethical, and sustainability obligations.
- Promptly notifying the Company of any actual or suspected noncompliance with this Code.
- Cooperating with the Company on investigations, audits, assurance activities, and corrective actions where required.
- Ensuring that equivalent standards are applied throughout their own supply chains where relevant.

Individual Responsibilities (Supplier Personnel)

Individuals working for or on behalf of Suppliers who are involved in providing goods or services to the Company are expected to:

- Act in a lawful, ethical, and professional manner always.
- Protect Company information and that entrusted to it, in accordance with agreed security and privacy requirements.
- Report concerns, breaches, or suspected misconduct in line with applicable whistleblowing or reporting arrangements.

Escalation and Accountability

Failure to meet the responsibilities outlined in this Code may result in corrective action plans, increased monitoring, suspension, or termination of the supplier relationship, depending on the nature and severity of the issue.

RACI table

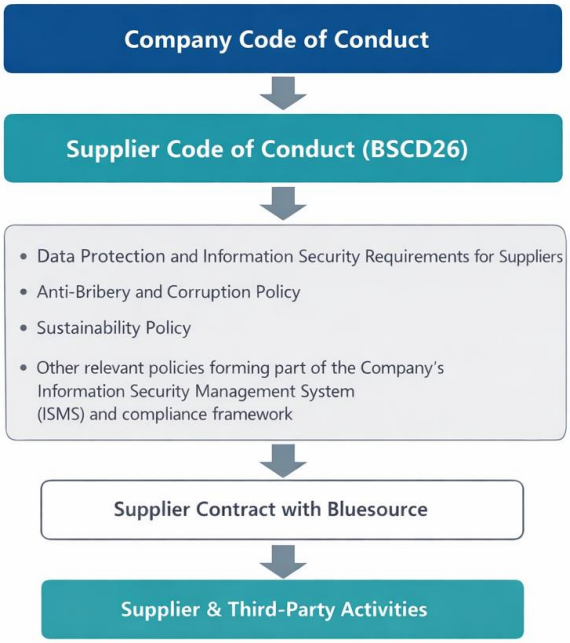
Activity	Head of Operations	IT / Operations	Supplier	Internal Audit / ISMS
Define and maintain Code	A/R	C	I	C
Communicate expectations	A	R	I	I
Supplier compliance	A	R	R	C
Monitoring & assurance	A	R	C	R
Investigation of breaches	A/R	R	C	C
Enforcement	A/R	C	I	C

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

9 Relationship with Company Policies and Supplier Contracts

This Supplier Code of Conduct forms part of the Company's wider governance, compliance, and contractual framework and must be read in conjunction with applicable Company policies and the relevant Supplier's contractual obligations.

The diagram below illustrates how this Supplier Code of Conduct aligns with Bluesource's governance framework, supporting policies, and supplier contractual arrangements.



Relationship with Company Policies

This Code establishes the minimum ethical, legal, and behavioural expectations for Suppliers. It is supported by a suite of Company policies and standards that define more detailed requirements in specific areas, including:

- **Company Code of Conduct** – overarching standards of behaviour and ethics applicable to all individuals and third parties;
- **Data Protection and Information Security Requirements for Suppliers** – detailed requirements relating to the protection of Company and customer information;
- **Anti-Bribery and Corruption Policy** – requirements relating to bribery, corruption, gifts, and hospitality;
- **Sustainability Policy** – environmental and responsible business commitments; and
- **Other relevant policies** forming part of the Company's Information Security Management System (ISMS) and compliance framework.

These policies operate together to form an integrated control environment supporting compliance with legal, regulatory, and contractual obligations.

Where requirements overlap, Suppliers must apply the higher ethical, legal, or compliance standard.

Relationship with Supplier Contracts

This Code is incorporated into, and forms part of, the contractual relationship between Bluesource and the Supplier, whether expressly referenced or implied through engagement.

Suppliers are required to:

- Comply with the provisions of this Code as a condition of doing business with Bluesource;

- Align their internal policies, controls, and practices with the expectations defined within this Code;
- Ensure that subcontractors and third parties engaged in the delivery of services to Bluesource are subject to equivalent contractual obligations; and
- Cooperate with Bluesource in demonstrating compliance with both this Code and applicable contractual requirements.

In the event of any inconsistency between this Code and a Supplier's contract:

- The contract shall prevail in respect of specific legal terms; however
- Suppliers must still meet the minimum ethical, security, and compliance standards defined in this Code unless otherwise formally agreed in writing.

Hierarchy of Requirements

The relationship between governance documents is structured as follows:

1. Legal and Regulatory Requirements (applicable laws and regulations);
2. Supplier Contract with Bluesource (binding legal agreement);
3. Company Code of Conduct (overarching ethical framework);
4. Supplier Code of Conduct (this document) (supplier-specific expectations);
5. Supporting Policies and Standards (detailed controls and procedures); and
6. Relevant statements of work (SOW) and/or service schedules.

This hierarchy ensures that Suppliers clearly understand how ethical expectations, contractual obligations, and operational controls interact within the Company's governance framework.

10 Acceptance and Acknowledgement

Compliance with this Supplier Code of Conduct forms part of the contractual relationship between the Company and the Supplier.

The Company may require formal acknowledgement of this Code as part of its governance and assurance processes.

11 Review and Revision

This Code is owned by the Head of Operations and is reviewed at least annually to ensure continued alignment with:

- Legal and regulatory requirements;
- UN Global Compact principles;
- Industry best practices; and
- Bluesource's governance and compliance framework.

12 Sign Off

For Bluesource	
Name	Nick Jaggers
Position	Head of Operations
Signature	
Date	8th May 2026

13 Revision History

Revision Date	Reviser	Description of Revision
12/03/2024	Nick Jaggers	Adapted from Bluesource's Corporate and Social Responsibility Policy.
08/03/2025	Nick Jaggers	No changes needed.
30/03/2026	Nick Jaggers	Review and alignment with UN Global Pact principles, ISO27001 and the Company's Sustainability Policy.
08/05/26	Nick Jaggers	Alignment made with new Company Code of Conduct to ensure consistency between the two documents.