Hybrid Working

Last updated 18 June 2026

1. Overview

Bluesource Information Limited (the "**Company**") operates a hybrid working model enabling employees to perform their duties both remotely and from Company premises, where appropriate.

This policy establishes the mandatory requirements, controls, and responsibilities governing hybrid working arrangements to ensure:

- Business continuity and operational effectiveness;
- Legal and regulatory compliance;
- Protection of Company and client information; and
- Employee health, safety, and wellbeing.

This policy applies to all employees engaged in hybrid or remote working arrangements and is for guidance only and does not form part of employees' contractual rights. The contents may be subject to revision from time to time and the policy may be withdrawn at any time with the Company not obligated to provide a reason as to why.

2. Purpose

The purpose of this policy is to:

- Define the conditions under which hybrid working is permitted;
- Ensure compliance with UK employment, health and safety, and data protection legislation;
- Align hybrid working practices with the Company's Information Security Management System (ISMS); and
- Support consistent, fair, and secure working practices across the organisation.

3. Scope

This policy applies to all employees engaged in hybrid or remote working arrangements across the Company.

It applies equally to all roles unless specific operational requirements or business needs dictate otherwise.

4. Definitions

For the purposes of this policy:

Hybrid Working – A working arrangement where employees perform their duties both remotely and at Company premises.

Remote Working – Working from a non-Company location, typically the employee's home.

Company Assets – All equipment, systems, devices, and information provided by or belonging to the Company for business use.

5. Regulatory and Standards Alignment

This policy is implemented in accordance with applicable UK legislation, including:

- Working Time Regulations 1998;
- Health and Safety at Work etc. Act 1974;
- Display Screen Equipment (DSE) Regulations;
- Equality Act 2010; and
- UK GDPR and Data Protection Act 2018.

This policy also aligns with recognised standards and frameworks, including:

- ISO/IEC 27001:2022 (Information Security Management System); and
- ISO/IEC 27002:2022 control framework.

In addition, the Company supports the principles of the United Nations Global Compact (UNGC), including:

- Principles 1–2: Protection of internationally proclaimed human rights; and
- Principles 3–6: Upholding labour rights, including freedom of association, elimination of forced labour, abolition of child labour, and elimination of discrimination in employment.

6. Applicability of other Company Policies and ISMS

This policy operates within the broader framework of the Company's policies, procedures, and Information Security Management System (ISMS). Hybrid working does not alter, replace, or reduce any obligations set out in these documents.

The following diagram provides an overview of the governance and control framework supporting hybrid working, demonstrating how this policy aligns with the Company's ISMS, regulatory obligations, and related policies.

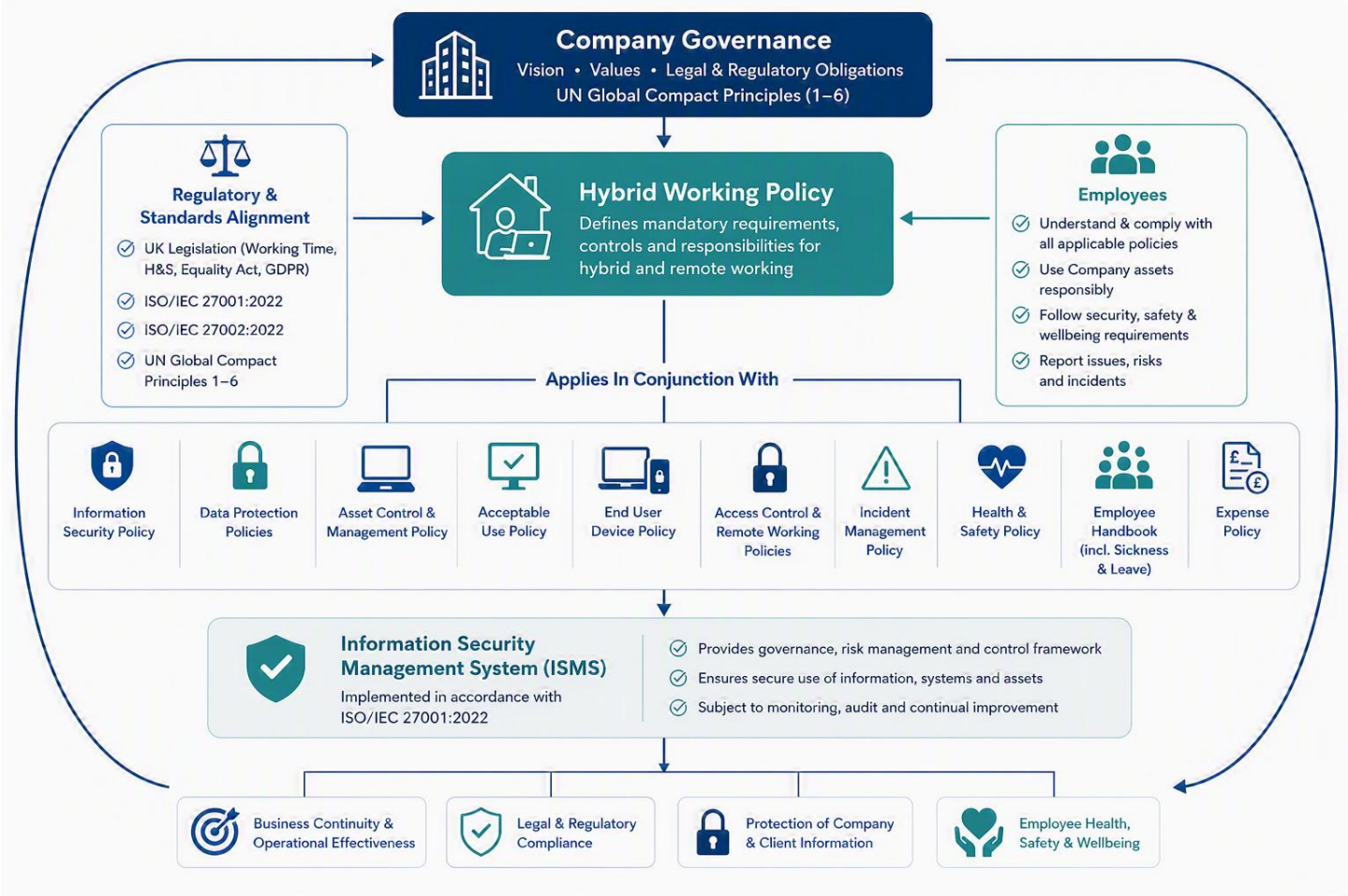

Figure - Hybrid Working Policy within the Company Governance and ISMS Framework

All employees must comply with all applicable Company policies when working remotely or under hybrid arrangements, including but not limited to:

- **End User Device Policy;**
- **Information Security Policy**;
- **Data Classification Policy**;
- **Asset Management Policy**;
- **Acceptable Use Policy**;
- **Access Control** and **Remote Working Policies**;
- **Incident Management Policy**;
- **Health and Safety Policy**;
- **Employee Handbook** (including Sickness and Leave Policies); and
- **Expense Policy.**

These policies apply equally and without exception to hybrid and remote working environments.

The Company's ISMS, implemented in accordance with ISO/IEC 27001:2022, defines the governance framework, control environment, and risk management processes supporting secure hybrid working. Employees are required to comply with all ISMS controls relevant to their role, including those relating to the secure use of information, systems, and Company assets.

In the event of any conflict between this policy and other Company policies, the requirements set out in the Company's Information Security, Data Protection, or Health and Safety policies shall take precedence where applicable.

Compliance with this policy and all referenced Company policies is mandatory for all employees engaged in hybrid or remote working arrangements.

Where more detailed requirements are defined in supporting policies, those policies shall take precedence and must be followed in full.

7. Roles and Responsibilities (RACI)

The following table defines the roles and responsibilities for the implementation, management, and oversight of hybrid working arrangements. This aligns with the Company's remote working practices and Information Security Management System (ISMS).

Activity / Control Area	Employees	Line Managers	HR	IT / Security	Operations	Senior Management
Hybrid working approval & suitability	I	R	C	I	A	I
Ongoing suitability (incl. relocation)	R	A	C	I	C	I
Working hours & availability compliance	R	A	C	I	I	I
Sickness & leave reporting	R	A	R	I	I	I
Provision of equipment	I	C	I	R	A	I
Asset control & inventory management	R	C	I	R	A	I
Acceptable use compliance	R	A	C	R	I	I
End user device security	R	I	I	A	C	I
Access control & remote system access	R	I	I	A	C	I
Information security & data protection	R	A	C	R	C	I
Incident identification & reporting	R	C	I	A	C	I
Incident response	I	I	I	R	A	I
Remote workspace safety (DSE, environment)	R	C	R	I	A	I
Health & safety risk assessments	I	C	R	I	A	I
Risk assessment & ISMS risk register	I	C	I	R	A	I
Expense approval & reimbursement	R	A	C	I	R	I
Policy compliance monitoring	I	C	C	C	R	A
Policy review & governance	I	I	C	C	R	A

Key:
R = Responsible (executes the activity)
A = Accountable (owns and approves the outcome)
C = Consulted (provides input)
I = Informed (kept updated)

8. Policy Principles

The Company's hybrid working model is based on:

- Flexibility balanced with business needs;
- Fair and non-discriminatory access;
- Trust supported by clear accountability;
- Secure use of technology and data; and
- Protection of employee wellbeing and safety.

9. Eligibility and Approval

Hybrid working is available to all employees unless deemed unsuitable based on:

- Role requirements necessitating full-time office presence;
- Inadequate or unsafe remote working environment;
- Insufficient connectivity or infrastructure;
- Performance or supervision concerns; or
- Business, client, or operational requirements.

9.1 Fairness and Equality

All decisions relating to hybrid working will be:

- Fair, transparent, and consistently applied;
- Made in accordance with the Equality Act 2010; and
- Supportive of reasonable adjustments where required.

9.2 Change in Circumstances (Including Relocation)

Hybrid working arrangements are subject to ongoing suitability. Employees must inform the Company of any material changes to their circumstances that may affect their ability to work remotely, including relocation or changes to their home working environment.

Where an employee moves home, the Company will reassess the suitability of the hybrid working arrangement. This may include consideration of health and safety requirements, workspace suitability, connectivity, and operational impact.

Where the Company determines that hybrid working is no longer appropriate following such reassessment, the arrangement may be amended or withdrawn in accordance with business needs.

10. Hybrid Working Arrangements

Hybrid working is granted at the discretion of the Company and may be varied, suspended, or withdrawn where required.

Employees must:

- Attend the office or other locations when requested;
- Support team collaboration, training, and client requirements; and
- Ensure their working arrangements do not negatively impact colleagues or service delivery.

11. Hours of Work and Availability

Employees must:

- Work contractual hours and days;
- Adhere to Flexible Working Policy provisions; and
- Comply with Working Time Regulations.

Including:

- Minimum 20-minute break per 6 hours;
- Minimum 11 hours daily rest; and
- Minimum one full day off per week.

Employees must report sickness absence and request leave in accordance with the Company's Sickness and Leave Policies, as detailed in the **Employee Handbook (Intranet)**. These requirements apply equally to hybrid and remote working arrangements.

Line managers are responsible for monitoring working patterns to ensure compliance and wellbeing.

Line managers should also consider employee wellbeing when monitoring working patterns, including workload, working hours, and signs of fatigue or stress.

12. Equipment and Asset Management

The Company will provide approved equipment required for hybrid working, including:

- Laptop (mandatory); and
- Company mobile phone (role dependent).

12.1 Asset Control

- All equipment remains Company property;
- Assets are recorded and managed within the Company asset inventory;
- Procurement must be authorised via the Operations team;
- All assets must always conform to Company security requirements (**see Section 13**);
- All assets must always be managed by the Company (such as via InTune); and
- All assets must be returned to the Company on request and on termination of employment.

All assets provided for hybrid working is subject to the Company's **Asset Management Policy (Intranet)** including requirements for asset registration, ownership, lifecycle management, maintenance, and return.

12.2 Acceptable Use

- Only Company-approved devices may be used to access systems and data; and
- Personal devices must not be used unless formally authorised in writing and secured with necessary controls.

All assets used under hybrid working are subject to the Company's acceptable use requirements, as outlined it its **Acceptable Use Policy (Intranet)**.

13. Information Security and Data Protection

All employees must comply with the Company's ISMS and data protection framework. All of the Company's Security Policies shall apply to remote working, including hybrid working.

13.1 Core Security Requirements

Employees must:

- Use only authorised, Company-managed devices;
- Protect credentials and use multi-factor authentication (MFA) where required;
- Access systems via secure and approved networks;
- Lock screens when unattended; and
- Ensure data is encrypted and securely stored.

For further information, please refer to the Company's **End User Device and Remote Working Policies (Intranet)**.

13.2 Prohibited Activities

Employees must not:

- Use unsecured or public networks without safeguards;
- Share devices with third parties; and
- Store Company data on unauthorised systems.

For further information, please refer to the Company's **Acceptable Use Policy (Intranet)**.

13.3 Information Handling

Employees must:

- Comply with data classification and retention policies;
- Prevent unauthorised disclosure or viewing of information; and
- Maintain a clear desk and screen policy.

Where physical documents are used, employees must ensure secure handling, storage, and disposal of printed materials in accordance with the Company's Information Security and Data Protection policies.

For further information, please refer to the Company's **Data Classification Policy (Intranet)**.

13.4 Incident Reporting

All security incidents, breaches, or weaknesses must be reported immediately in accordance with the **Incident Management Policy (Intranet)**.

14. Remote Working Environment

Employees are responsible for maintaining a workspace that is:

- Safe and ergonomically suitable;
- Secure from unauthorised access; and
- Free from distraction and appropriate for work.

Employees must not:

- Disclose homeworking status to clients where inappropriate;
- Share personal contact details or addresses; and
- Host business meetings at home without approval.

15. Remote Workplace Access

The Company may, where reasonably necessary and with prior agreement, arrange access to an employee's remote working environment for legitimate work-related purposes, including health and safety assessments, equipment inspection, or risk management activities.

Any such access will:

- Be conducted with reasonable notice;
- Require the employee's prior agreement;
- Be limited to areas relevant to work activities; and
- Be proportionate and respectful of the employee's privacy.

Where physical access is not appropriate, alternative arrangements such as self-assessment or virtual review may be used.

16. Health, Safety and Wellbeing

The Company will ensure, so far as reasonably practicable, the health, safety, and welfare of hybrid workers.

16.1 Employer Responsibilities

The Company will:

- Conduct risk assessments;
- Provide training and guidance;
- Ensure equipment safety and suitability; and
- Support employee wellbeing, including mental health.

16.2 Employee Responsibilities

Employees must:

- Follow all health and safety guidance;
- Maintain a safe workstation; and
- Report accidents, hazards, or concerns.

16.3 DSE Compliance

Employees must ensure proper use and positioning of display screen equipment in line with DSE requirements. Further guidance is provided in the **Employee Handbook (Intranet)**.

17. Risk Assessment

Remote working risks are assessed through:

- Initial and periodic risk assessments; and
- Self-assessment where appropriate.

Identified risks are:

- Recorded within the ISMS risk register where appropriate and information security related; and
- Managed through the Company's risk treatment process.

18. Expenses and Costs

The Company will not ordinarily reimburse:

- Utilities (electricity, heating, broadband); and
- General homeworking costs.

Any work-related costs, including printing or postage where required, must be pre-approved and claimed in accordance with the Company's **Expense Policy (Intranet)**.

19. Communication and Collaboration

Employees must:

- Maintain regular contact with line managers and teams;
- Attend required meetings, including Company-wide sessions; and
- Use approved communication platforms (e.g., Microsoft Teams).

HR and IT support remain available via email or phone.

The Company has a weekly "all-hands" Teams video call, typically on a Friday, so that all employees can keep in regular contact with one another at a Company level and can interact with what is going on in all departments. Unless otherwise engaged on urgent work-related business, it is expected that all employees should attend, with video on. A background, ideally the Company provided backdrop, can be used to obscure the personal workspace.

20. Office Working Requirements

When attending Company premises, employees must:

- Follow all security and access control procedures;
- Prevent unauthorised access ("tailgating");
- Take responsibility for visitors;
- Maintain cleanliness, safety, and professional standards;
- In the absence of a designated fire marshal in the office, the meeting chairperson and most senior person onsite must perform fire marshalling duties and report back to Operations. Fire marshal/warden training is provided to all members of staff to facilitate this
- If necessary, procure items for daily consumption such as milk and bread, claiming on expenses where appropriate;
- Report facility issues to Operations; and
- Must leave the office secure.

21. Insurance and Personal Responsibilities

Employees are responsible for ensuring:

- Home and contents insurance covers remote working; and
- Mortgage or tenancy agreements permit working from home.

The Company accepts no liability for personal property or related costs.

22. Monitoring, Compliance and Enforcement

Compliance with this policy will be:

- Monitored by Operations, HR, and Management; and
- Subject to audit under the ISMS framework.

Non-compliance may result in:

- Withdrawal of hybrid working arrangements; and
- Disciplinary action in line with Company policy.

Any issues, non-compliance, or control weaknesses identified through monitoring or audit activities will be managed in accordance with the Company's corrective action and continuous improvement processes.

23. Review and Governance

This policy is owned by the Head of Operations and approved by Senior Management.

The policy will be:

- Reviewed at least annually;
- Reviewed following any significant legal, regulatory, operational, or organisational change; and
- Updated where required to ensure continued effectiveness and compliance.

This policy forms part of the Company's wider governance framework and supports the Information Security Management System (ISMS) implemented in accordance with ISO/IEC 27001:2022.

Compliance with this policy, and its ongoing suitability, will be considered as part of the Company's ISMS monitoring and Management Review activities.

Any material changes to this policy must be approved in accordance with the Company's governance and change management processes.

The Head of Operations is responsible for ensuring that this policy is maintained, reviewed, and updated in line with Company governance requirements, including version control and distribution.

24. Acceptance

Hybrid working arrangements are subject to acceptance of this policy. Continued participation in hybrid working constitutes agreement to comply and acceptance of this Policy.

25. Sign-Off

For Bluesource	
Name	Nick Jaggers
Position	Head of Operations
Signature	
Date	16 June 2026

26. Revision History

Revision Date	Reviser	Description of Revision
29/06/2021	Nick Jaggers	Draft
13/09/2021	Nick Jaggers	Initial publication.

09/09/2022	Nick Jaggers	Reviewed and no amendments required
09/06/2023	Nick Jaggers	Reviewed and no amendments required
21/06/2024	Nick Jaggers	Rebranded and updated.
24/06/2025	Nick Jaggers	Reviewed and no changes.
16/06/2026	Nick Jaggers	Annual review and revision. RACI and applicability of other policies added.