Information Security Statement

Version 1.0
Last Reviewed: May 2026

Purpose

At Bloomfield Street, information security is fundamental to the way we operate. We recognise that clients trust us with sensitive operational, commercial and organisational information, and we are committed to protecting that information through practical, proportionate and risk-based security practices.

As an operational infrastructure partner, we understand that effective information security is not simply a technical exercise. It is an essential part of resilient operations, responsible governance and sustainable business growth.

This statement outlines Bloomfield Street's commitment to protecting the confidentiality, integrity and availability of the information we process, store and access as part of our business activities.

Our Commitment

Bloomfield Street is committed to maintaining appropriate technical, organisational and administrative safeguards to protect information against unauthorised access, disclosure, alteration, loss or destruction.

Our approach is informed by recognised UK and European legal, regulatory and good practice principles, including:

- UK General Data Protection Regulation (UK GDPR)
- EU GDPR principles where applicable
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Security practices informed by Cyber Essentials principles
- Risk management and information security practices informed by ISO 27001 principles
- Privacy by Design and Default principles

While Bloomfield Street is not currently formally certified against Cyber Essentials or ISO 27001, we are committed to developing our security maturity over time and continually strengthening our governance, operational controls and cyber security practices in line with recognised frameworks and business growth.

Information Security Principles

Risk-Based and Proportionate Security

Bloomfield Street applies security measures appropriate to the size, nature and operational requirements of the business. Our approach is designed to reduce risk while maintaining practical, efficient and sustainable operations.

Information security considerations are embedded into operational decision making, supplier onboarding, system selection, process design and service delivery activities.

Protection of Information

We are committed to protecting information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

This applies to all information processed by Bloomfield Street, including:

- Personal data
- Commercial information
- Operational records
- Client documentation
- Confidential communications
- Financial and supplier information

Secure Systems and Technology

Bloomfield Street operates a cloud-first technology environment using carefully selected platforms and providers to support secure and effective business operations.

Security measures include, where applicable:

- Company-managed devices
- Device password and screen lock requirements
- Multi-factor authentication (MFA)
- Role-based access controls
- Least privilege access principles
- Controlled user access reviews
- Access removal processes when access is no longer required
- Microsoft 365 based document and information management
- Secure cloud storage practices
- Use of approved systems and software providers
- Secure handling of sensitive information within approved storage environments
- Regular software and platform updates through supported systems and providers

Sensitive information is stored within approved business systems and environments. Bloomfield Street intentionally separates highly sensitive information from general operational platforms where appropriate to support effective risk management and data minimisation practices.

Access Control and User Responsibility

Access to information is restricted to authorised individuals who require access for legitimate business purposes.

Bloomfield Street expects employees, contractors and associates where applicable to:

- Handle information responsibly
- Follow secure working practices
- Protect confidential information
- Maintain appropriate password and authentication standards
- Report suspected security concerns promptly

Shared accounts and unnecessary access permissions are avoided wherever possible.

Supplier and Third Party Security

Bloomfield Street works with selected third party providers to support operational delivery, communication, hosting, scheduling, analytics and business administration activities.

We undertake proportionate due diligence and security considerations before onboarding new suppliers or systems, including consideration of:

- Data protection obligations
- Security practices
- Hosting arrangements
- Access controls
- Operational risk
- Appropriate contractual protections where required

Third party suppliers are expected to maintain appropriate standards of security and confidentiality relevant to the services they provide.

Incident Management and Breach Response

Bloomfield Street maintains procedures for identifying, managing and responding to information security incidents and potential personal data breaches.

Incidents are assessed appropriately, documented where necessary and managed in line with applicable legal and regulatory obligations. Where required, personal data breaches will be reported to the appropriate supervisory authority and affected individuals in accordance with UK GDPR and related legislation.

Business Continuity and Operational Resilience

Bloomfield Street recognises that operational resilience forms part of effective information security. We maintain proportionate business continuity and operational resilience arrangements designed to support continuity of service, protection of information and recovery from disruption where reasonably possible.

Cloud-based systems and operational processes are selected with resilience, continuity and secure access considerations in mind.

Monitoring, Review and Continuous Improvement

Information security is an ongoing operational responsibility rather than a one-time exercise.

Bloomfield Street is committed to regularly reviewing and improving its information security practices to reflect:

- Emerging cyber threats

- Business growth and operational change
- Technology developments
- Regulatory changes
- Lessons learned from incidents or reviews
- Evolving good practice standards

We aim to maintain a practical, transparent and continuously improving approach to information security that supports safe, effective and sustainable operations.

Scope

This statement applies to all information processed by Bloomfield Street in connection with its business activities, regardless of format, including digital, physical and verbal information.
It applies to all employees, contractors and associates working for or on behalf of Bloomfield Street where applicable.

Review

This statement will be reviewed annually, or earlier where required due to:

- Significant business or operational change
- Changes in applicable legislation or regulation
- Changes to technology or systems
- Security incidents or identified risks
- Changes to organisational structure or service delivery