JUSTMATTER

Confidentiality and Data Protection Policy

Version: 1.0
Release Date: January 2026

Contents

1. Purpose and Commitment

Just Matter recognizes that confidentiality and data protection are fundamental to the credibility of assurance and auditing activities. The firm routinely receives access to sensitive commercial, operational, personal, and strategic information, including information that, if mishandled, could result in financial harm, regulatory exposure, reputational damage, risk to personal safety or loss of trust for clients and other stakeholders.

This policy sets out the principles, responsibilities, and controls through which Just Matter protects information entrusted to it. It establishes a structured approach to confidentiality and data protection that supports professional independence, audit quality, and compliance with recognized information security management standards. The policy is designed to ensure that information is protected throughout its lifecycle, from initial collection through use, storage, sharing, retention, and secure disposal.

2. Scope of Application

This policy applies to all information created, received, accessed, processed, or stored by Just Matter in connection with its business activities. This includes, but is not limited to, audit evidence, working papers, client documentation, correspondence, internal methodologies, commercial information, personal data, and system-generated data.

The policy applies regardless of the medium in which information exists, including electronic systems, cloud platforms, physical documents, portable devices, verbal communications, and visual displays. It applies equally to routine business operations and to information obtained during assurance engagements, pre-engagement activities, complaints handling, or internal governance processes.

All individuals acting on behalf of Just Matter are subject to this policy. This includes directors, employees, independent contractors, subcontract auditors, associates, and any other parties granted access to Just Matter information systems or records.

3. Definitions and Interpretation

For clarity and consistency, key terms used in this policy are defined and interpreted broadly to ensure protection is not limited by technical distinctions.

Confidential information includes any non-public information relating to clients, audited entities, Just Matter's operations, or third parties, whether marked as confidential or not, where a reasonable expectation of confidentiality exists.

Personal data includes any information relating to an identified or identifiable natural person, whether held directly or indirectly, and regardless of jurisdiction-specific terminology used in applicable data protection laws.

Processing refers to any action performed on information or data, whether automated or manual, including collection, recording, organization, storage, consultation, analysis, transmission, retention, or destruction.

4. Fundamental Confidentiality Principles

Just Matter treats all information obtained in the course of professional activities as confidential by default. Information is used strictly for legitimate business and assurance purposes and only to the extent necessary to perform agreed services or meet legal and professional obligations.

Confidential information is not disclosed to third parties without a valid and documented basis. Such bases may include client authorization, contractual necessity, regulatory or accreditation requirements, or legal compulsion. Where disclosure is required, Just Matter limits the scope of disclosure to the minimum necessary and applies appropriate safeguards.

Confidentiality obligations survive the completion of an engagement and the termination of any contractual or employment relationship. Individuals remain bound by confidentiality requirements indefinitely unless information has lawfully entered the public domain through no fault of Just Matter.

5. Data Protection and Privacy Principles

Just Matter processes personal data in a manner that is lawful, fair, and transparent. Individuals whose personal data is processed are treated with respect, and data is handled in a way that reflects its sensitivity and potential impact.

Personal data is collected only where there is a clear professional, contractual, or legal purpose, and only data that is relevant and necessary for that purpose is processed. Just Matter avoids collecting excessive or speculative personal data and seeks to anonymize or aggregate data where feasible.

Personal data is maintained accurately and updated where necessary to support assurance activities and governance requirements. Inaccurate or outdated personal data is corrected or deleted as soon as reasonably practicable once identified.

6. Lawful Basis and Purpose Limitation

All processing of personal data by Just Matter is supported by a lawful basis, such as contractual necessity, legal obligation, legitimate professional interest, or explicit consent where required. Data is not processed for purposes that are incompatible with the original reason for collection.

Where data is reused for secondary purposes, such as quality reviews, accreditation assessments, or internal monitoring, Just Matter ensures that such use is compatible with the original purpose and subject to appropriate safeguards.

7. Information Classification Framework

To ensure proportionate protection, Just Matter classifies information based on its sensitivity, criticality, and potential impact if compromised. Classification guides decisions regarding access controls, storage, transmission, and disposal.

At a minimum, information is classified into categories such as public, internal, confidential, and highly confidential. Audit working papers, client data, personal data, and proprietary methodologies are typically classified as confidential or highly confidential and subject to enhanced controls.

Classification is applied at the time information is created or received and is reviewed as information changes in sensitivity over time.

8. Access Control and Authorization

Access to information is granted strictly on a need-to-know basis. Individuals are provided with the minimum level of access necessary to perform their assigned responsibilities, and access rights are approved and documented.

User access to electronic systems is controlled through unique user accounts, strong authentication measures, and role-based permissions. Shared accounts are avoided except where operationally unavoidable and explicitly authorized.

Access rights are reviewed periodically and promptly updated when roles change, engagements conclude, or individuals leave the organization.

9. Physical and Environmental Security

Physical records and devices containing confidential or personal data are protected against unauthorized access, loss, or damage. Secure storage arrangements are used for sensitive documents, and access to physical workspaces is controlled where appropriate.

Environmental risks such as fire, water damage, or theft are considered in determining storage and handling arrangements. Reasonable measures are taken to prevent accidental exposure of confidential information in shared or public spaces.

10. Information Security and Technical Controls

Just Matter implements technical and organizational controls designed to preserve the confidentiality, integrity, and availability of information throughout its lifecycle. These controls are risk-based and proportionate to the sensitivity of information handled, the nature of assurance engagements, and the firm's operating model as an independent ESG assurance provider.

Electronic information is stored and processed using secure, reputable information systems and cloud-based platforms that incorporate recognized information security management practices. Where feasible and appropriate, Just Matter uses data storage, document management, and collaboration systems that are hosted within environments certified to ISO/IEC 27001 or equivalent internationally recognized information security standards. Reliance on ISO/IEC 27001–certified hosting environments provides assurance that such systems operate within a structured information security management framework, including controls over access management, physical and environmental security, incident management, and business continuity.

Just Matter does not rely solely on third-party certifications as a substitute for its own controls. System configurations, access permissions, and user management are administered by Just Matter to ensure that confidentiality requirements specific to assurance engagements are met. Access to systems is restricted through role-based permissions, strong authentication measures, and regular access reviews to ensure that only authorized individuals can access confidential or personal data.

Technical safeguards include, where appropriate, encryption of data at rest and in transit, secure backup and recovery arrangements, malware and threat protection, and audit logging to support traceability and accountability. Systems used for audit delivery and evidence management are selected and configured to support version control, data integrity, controlled collaboration, and defensible audit trails.

Information security controls are reviewed periodically in light of changes in technology, emerging threats, professional standards, and regulatory expectations. Where new systems or tools are introduced, security considerations are assessed prior to use to ensure continued alignment with this policy and with recognized information security best practices.

11. Remote Working and Mobile Information Handling

Remote working arrangements are designed to maintain the same level of confidentiality and data protection as office-based work. Personnel are required to ensure that confidential information is not accessible to unauthorized individuals when working remotely.

Reasonable precautions are taken to protect information during travel, including the secure use of devices, avoidance of unsecured networks, and safeguarding of physical documents. Portable storage devices are used only where necessary and are subject to additional controls.

12. Third-Party and Subcontractor Controls

Where third parties or subcontract auditors process information on behalf of Just Matter, the firm ensures that confidentiality and data protection obligations are clearly defined and contractually enforced.

Due diligence is performed prior to granting access to sensitive information, considering the third party’s security controls, competence, and reliability. Access is limited to what is necessary, time-bound where possible, and subject to monitoring.

13. Data Retention and Lifecycle Management

Just Matter maintains documented retention periods for different categories of information, reflecting professional standards, legal requirements, contractual obligations, and accreditation expectations.

Information is retained only for as long as necessary to support assurance defensibility, regulatory compliance, and legitimate business needs. At the end of the retention period, information is securely deleted, destroyed, or anonymized in a manner appropriate to its classification.

14. Data Breach and Security Incident Response

Just Matter maintains procedures to identify, report, assess, and respond to suspected or actual information security incidents, including data breaches. All personnel are required to report incidents promptly, regardless of perceived severity.

Incidents are investigated to determine root cause, impact, and required corrective actions. Where notification is required by law, contract, or professional obligation, Just Matter communicates transparently with affected parties and relevant authorities within required timeframes.

15. Training, Awareness, and Professional Responsibility

All individuals acting on behalf of Just Matter are required to understand and comply with this Confidentiality and Data Protection Policy and with any related information security, privacy, and confidentiality procedures applicable to their role. Adherence to these requirements is a core professional obligation and forms part of the firm's commitment to audit quality, independence, and ethical conduct.

Just Matter ensures that personnel are provided with appropriate guidance and awareness to understand confidentiality and data protection expectations, particularly in the context of assurance engagements involving sensitive ESG, operational, and personal information. This includes awareness of risks associated with electronic systems, remote working arrangements, and the handling of audit evidence and working papers.

Personnel are expected to exercise professional judgment, diligence, and caution when handling confidential information and personal data, including identifying potential confidentiality risks and escalating concerns where uncertainty exists. Individuals must not assume that convenience, operational pressure, or client expectations justify departures from established confidentiality or data protection requirements.

Compliance with this policy is monitored through engagement oversight, quality management processes, and management review. Failure to comply with confidentiality and data protection requirements may result in disciplinary action, removal from engagements, or other appropriate measures.

16. Client Information Systems Requirements

Just Matter frequently performs assurance and auditing activities within information systems, platforms, and environments that are owned, operated, and controlled by clients or audited entities. These client information systems may include document repositories, audit portals, enterprise platforms, data rooms, and other controlled environments subject to client-defined security, access, and usage requirements.

All personnel acting on behalf of Just Matter are required to understand and comply with client-established confidentiality, data protection, and information security requirements applicable to such systems. This includes, without limitation, client policies governing access authorization, authentication methods, monitoring, data classification, data extraction, copying, transmission, retention, and destruction.

Access to client information systems must be used solely for authorized engagement purposes and strictly within the scope of permissions granted by the client. Personnel must not attempt to bypass, disable, weaken, or otherwise circumvent client-implemented technical, administrative, or procedural controls, even where such controls may be perceived as restrictive or inefficient.

Client data accessed during an engagement must not be transferred, replicated, stored, or processed outside client-approved systems unless explicitly authorized by the client and consistent with contractual, legal, and professional obligations. Where Just Matter systems are used to store or process client data, such use must be documented, justified, and subject to appropriate safeguards.

Where client requirements are unclear, inconsistent, or appear to conflict with professional obligations or this policy, personnel are required to escalate the matter to Just Matter management for resolution before proceeding. Under no circumstances should individuals make unilateral decisions to override client-defined controls or security requirements.

Compliance with client information system requirements is monitored through engagement oversight, quality review, and management controls. Breaches of client system requirements or attempts to circumvent client controls may result in disciplinary action, removal from engagements, contractual consequences, and potential legal or regulatory exposure for both the individual and Just Matter.

17. Governance, Oversight, and Continuous Improvement

Senior management retains overall accountability for confidentiality and data protection. Responsibilities are supported through defined roles, internal oversight, and integration with quality and risk management processes.

This policy is reviewed periodically to ensure ongoing suitability, effectiveness, and alignment with professional standards, regulatory expectations, and the firm's operating environment. Improvements are implemented where gaps or emerging risks are identified.

18. Non-Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action, contractual consequences, or termination of engagement. Serious or deliberate breaches may expose individuals and the firm to legal, regulatory, or reputational consequences.

Just Matter treats breaches of confidentiality and data protection as serious professional matters and responds accordingly.