Information Security policy

Document owners: **Business Information security officer** **Data Protection Compliance Manager**	Effective date: *01/05/24*
Accountable Group Leadership Team member: Members of the R&CSC	Due next review: *31/04/27*

Version No	Date	Reason for change:
1.0	April 2024	New document
2.0	July 2026	Review; minor tweaks

Purpose

Information is a vitally important corporate asset which requires protection against risks which would threaten its confidentiality, integrity and availability. This policy and associated standards, requirements and procedures are intended to provide the framework for ensuring adequate protection of all information assets and processing operations. It is designed to ensure the confidentiality, integrity and availability of the data or information we process and share, minimising the risk of security incidents and reducing their potential impact.

BMJ Group recognises the additional security and compliance measures that need to be in place when processing sensitive personal information. BMJ Group has developed further policies covering Data Protection and Information Classification in support of that. The controls identified in those policies will ensure the security of our information assets and provide overall assurance for both BMJ Group and our customers. The Executive Board and Management of BMJ Group are committed to managing the confidentiality, integrity and availability of all physical and electronic information assets throughout the organisation through the deployment of robust information security management and assurance.

Confidentiality	is ensured by having in place a suite of policies and procedures that limits access to both sensitive corporate and personal information.
Integrity	is the assurance that the information is trustworthy and accurate and covers data quality.
Availability	is a guarantee of ready access to the information by authorised people.

Scope

This policy applies to any data or information that is held, obtained, recorded, used, shared and archived or destroyed by BMJ Group irrespective of whether it is held in electronic or paper format.

It applies to all members of staff, permanent or temporary, including fixed and long-term contractors (staff), BMJ Data Processors, freelancers, sub-contractors, secondees, volunteers etc. The standards and

requirements shall have effect irrespective of the time or location the staff member is working and as such are applicable when working in a normal office or other remote environments.

Implementation

BMJ Group has committed to:

1	Continuous improvement initiatives, including appropriate and timely audit, risk assessment and risk management strategies. Maintain compliance with its policies and applicable global legislation and regulation. Communicate its Information Security and Governance policies, standards and objectives throughout the business and to other relevant parties by using appropriate training and awareness methods: ● training is conducted as part of induction; ● training material and policies are made available on the company's intranet; and ● self-certification is required every two years.
2	Ensure that all Information Security incidents are investigated and followed up.
3	Liaise with and share good practice with customers, business partners and other relevant parties to further promote Information Security and Governance standards.
4	Produce suitable and effective Business Continuity Plans with a robust testing structure.

Who is responsible, and for what?

Everybody working for BMJ Group (permanent or temporary staff, business partners, third party suppliers, contractors, freelancers, vendors, temps, consultants, interns, etc.) who has access to BMJ Group information worldwide, must adhere to this policy and are responsible for implementing and maintaining BMJ Information Security and Governance standards. This is irrespective of the time or location, when working in a normal office or other remote environments.

In addition:

1	The further development of this policy and any accompanying procedures will be the responsibility of the Information Governance Steering Committee.
2	The company operates a process of continual training and ongoing review of all security guidelines, with an emphasis on creating a culture which recognises the importance of information governance.
3	Senior Managers (members of the Group and Senior Leadership teams) will be responsible for their own specific area and in some circumstances will be Policy Owners, responsible for review, update and cascading their policies, procedures and standards to all staff covered and expected to implement the policy.
4	All Staff must be aware of and comply with the requirements of the Information Security and Governance policies, procedures and standards.

Why is this policy needed?

The management of BMJ Group is committed to the adoption and continuous development of appropriate and relevant information security controls to meet the highest possible standards of information security.

The primary reasons for this are twofold:

1	In support of BMJ values,
2	The legal and regulatory requirements BMJ Group must adhere to, such as and not restricted to:

	• The Data Protection Act 2018 • The General Data Protection Regulation • Privacy and Electronic Communication Regulations • The Computer Misuse Act 1990 • The Human Rights Act 1998 Plus, where relevant, the standards as published by the: • Information Commissioner's Office • British Standards Institute (BSI): Standards ISO 27001

Exemptions

Any deviation from this policy must be documented, risk assessed and agreed by the Information Governance Steering Committee, Risk & compliance steering committee or a nominated representative.