DATA PROTECTION AND PRIVACY POLICY

M&S is committed to complying with all applicable data protection and privacy legislation when collecting and using personal data of customers, colleagues and others. In summary, this means we:

(i) keep personal data secure and protected against unauthorised access or disclosures;

(ii) handle personal data in a fair and transparent manner; and

(iii) respect the privacy and data protection rights of individuals.

OUR KEY PRINCIPLES

WHY IS PERSONAL DATA IMPORTANT?

As a large retail business with millions of customers and thousands of colleagues in the UK and overseas, M&S collects and handles large volumes of personal data. This is necessary for us to run our business, including managing colleagues, keeping our customers safe and trading in our stores and online. Effective use of personal data is particularly important to ensure we offer and supply products which best meet our customers' needs and become a fully data driven and digital business. We recognise that whilst personal data is a critical business asset, we must utilise it in a way which respects individuals' rights and complies with our legal duties.

M&S is committed to complying with all applicable data protection laws and keeps fully abreast of all guidance issued by the data protection regulators.

Any breach of our legal obligations can have very serious consequences including:

- exposing customers and colleagues to damage and distress;
- enforcement action and multi-million pound fines being imposed on M&S; and
- loss of customer goodwill and trust.

DUTIES AND RESPONSIBILITIES

Colleague responsibilities

All colleagues have a personal responsibility to help M&S comply with data protection laws. In particular, colleagues must comply with our **Data Protection Policy for Colleagues** (available on the Knowledge Base in My HR and on the Data Protection Team Hub on M&S World) and ensure they complete mandatory data protection training each year.

The Data Protection Policy for Colleagues provides clear guidance on how personal data must be treated, identifies key do's and don'ts, and contains information about where to get further advice and how to report or escalate issues.

Colleagues must also comply with the **Acceptable Use Policy** which sets out the rules on appropriate and safe use of M&S systems and/or devices and on the acceptable use of Artificial Intelligence Technology in the workplace.

Data Protection Officer's team

The M&S Data Protection Officer ("DPO") and team ("the DPO team") is responsible for ensuring that appropriate compliance controls and procedures are in place. The DPO team is supported by a network of Data Compliance Managers embedded across our business who are responsible for day-to-day compliance.

The DPO team is also responsible for responding to requests by customers, employees and other individuals exercising their data protection rights. The DPO team works closely with the Cyber Security team to ensure appropriate data security controls are applied to personal data.

Transparency and fair processing

To comply with our duties to process personal data in a fair and transparent manner, and comply with individuals' rights, we provide appropriate data privacy notices explaining how personal data is used by M&S. The two main notices for customers and employees are the **M&S Customer Privacy Notice** (published on our customer website) and the **M&S Colleague Privacy Notice** (available on the Knowledge Base in My HR and on the Data Protection Team Hub on M&S World) respectively.

Suppliers and service providers

We require any supplier, service provider or other third party that processes personal data on behalf of M&S (defined as a "data processor") to enter into a contract which includes appropriate data protection provisions. This includes the legal clauses required under the GDPR as well as more detailed data security obligations where appropriate. Our Cyber Security team will also conduct pre-contractual due diligence and subsequent audits where appropriate, in order to provide assurance on data security.

DATA PROTECTION AND PRIVACY POLICY

Information Security Management

Our Cyber Security team operate to maintain appropriate data security controls for personal data and the systems in which it is held. This includes monitoring and assessing threats and responding to attempted attacks on our systems. We have procedures in place to manage data security incidents appropriately, including making appropriate notifications to regulators where required. We also conduct data security breach exercises on a regular basis.

COMPLIANCE

All colleagues must comply with the relevant policies and any failure to do so will be treated seriously. Non-compliance may result in disciplinary procedures up to and including dismissal.

We monitor compliance using a range of measures including:

- Training completion statistics
- Complaints by customers, employees and others
- Investigations by data protection regulators
- Queries and requests for advice
- Assurance activities undertaken by our Data Compliance Managers, including conducting Data Protection Impact Assessments which identify risks and mitigating actions.

REPORTING AND QUERIES

If you have data protection queries, concerns or need advice, please contact the Data Compliance Manager for your business unit or the DPO's team by emailing DataProtectionOfficer@marks-and-spencer.com.

If you believe there has been a breach of M&S data security resulting in access to, or loss of personal data held in our systems (or those operated for us by third parties) please report this to the Cyber Security team immediately by either of the following:

- Email: cyber.security@marks-and-spencer.com
- Telephone: **+44 (0) 2087 185999**

FURTHER GUIDANCE DOCUMENTS

The DPO team maintains a Knowledge Hub on M&S World which contains data protection guidance on specific topics and for specific Business units. Guidance is also available for store colleagues guidance on the M&S MySafety app.

FURTHER INFORMATION

Policy Owner	General Counsel
Compliance Lead	Data Protection Officer
Published / Effective from	January 2026
Review frequency	Annually
Next review date	January 2027