DATA PROTECTION AND PRIVACY POLICY

OUR KEY PRINCIPLES

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.

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 employees, 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 including:

- UK General Data Protection Regulation; and
- Data Protection Act.

M&S keeps fully abreast of all guidance issued by the UK's data protection regulator, the Information Commissioner's Office.

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

- exposing customers and employees 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 and Privacy laws. In particular, colleagues must comply with our **Data Protection Policy for colleagues**, 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.

Data Protection Officer's team

M&S appointed a Data Protection Officer ("DPO") before the GDPR came into force, and the DPO's team is principally responsible for ensuring that appropriate compliance controls and procedures are in place. The DPO is supported by a Deputy DPO and a network of 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 provided in the **M&S Privacy Policy** (published on our customer website) and the **M&S Colleague Privacy Policy** (published on our intranet site) 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

DATA PROTECTION AND PRIVACY POLICY

appropriate. Our Cyber Security team will also conduct pre-contractual due diligence and subsequent audits where proportionate, in order to provide assurance on data security.

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 the ICO
- Queries and requests for advice
- Assurance activities undertaken by our 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 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: cybersecurityoperations@mnscorp.onmicrosoft.com
- Telephone: 0044 2087 185151

FURTHER GUIDANCE DOCUMENTS

Please refer to the following documents, published on the People Hub section on the intranet, for further information:

- **Data Protection Policy** for colleagues
- **Acceptable Use Policy**

FURTHER INFORMATION

Policy Owner	General Counsel
Compliance Lead	Data Protection Officer
Published / Effective from	March 2024
Review frequency	Annually
Next review date	March 2025