

Data Protection Policy



Policy Overview

This policy sets out how we process the personal data that we hold (relating to colleagues, customers, suppliers and other third parties). It outlines our responsibilities under data protection legislation and regulations, setting out how we will comply and provide instruction for colleagues handling personal data.

Version/issue:	Issue 8
Ratified by:	Chief Legal Officer
Date ratified:	4 December 2025
Author/originator:	Chief Legal Officer
Developed in association with:	N/A
Review date:	December Annually
Name of responsible reviewer:	Senior Legal Counsel

When this document is viewed as a paper copy, the reader is responsible for establishing that it is the most current version.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

12/2025 – Issue 8

Marshalls

Data Protection Policy



1. Policy Statement

- 1.1. This Data Protection Policy is issued by and on behalf of the Marshalls group of companies. The Marshalls group of companies is made up of different legal entities, including Marshalls plc, Marshalls Group Limited, Marshalls Mono Limited, Marley Limited, and Viridian Solar Limited. When we say "Marshalls", "the Company", "we", "us" or "our" in this policy, we are referring to the relevant company in the Marshalls group of companies responsible for processing personal data.
- 1.2. Everyone has rights with regard to how their personal data is handled.
- 1.3. During the course of our activities, Marshalls will collect, store and process personal data about our customers, suppliers, and other individuals with whom we communicate. This may include personal data we receive directly from those individuals (for example, where a customer makes an enquiry about or orders any of our products and/or services), data we gather ourselves (for example from CCTV), or data we receive from other sources (including, for example, credit reference agencies, business partners, service providers and others).
- 1.4. Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation EU 2016/679 (UK GDPR), the Data Protection Act 2018, as well as other data protection and privacy laws such as the Privacy and Electronic Communications (EC Directive) Regulations 2003 as may be updated or replaced from time to time (the "**Data Protection Laws**"). The enforcement of Data Protection Laws in the UK is regulated by the Information Commissioner's Office (the ICO) - you can find out more at www.ico.org.uk.
- 1.5. We recognise that the fair, transparent and lawful treatment of this data will maintain confidence in Marshalls. This policy sets out our rules on data protection and the legal requirements that must be satisfied by Marshalls and our colleagues in relation to the obtaining, handling, use, storage, transfer and destruction and other processing of such personal data.
- 1.6. This policy applies to all Data Users (as defined below). All Data Users should familiarise themselves with this policy and comply with its terms when processing personal data on behalf of Marshalls in the course of their employment.
- 1.7. This policy does not form part of any colleague's contract of employment and may be amended by us at any time.
- 1.8. Any breach of Data Protection Laws can expose Marshalls to significant financial penalties and reputational damage, but it can also extend to you individually, which is why it is important that you understand and comply with this policy when processing personal data.

2. Definition of Data Protection Terms

Criminal Convictions Data: Personal data relating to criminal convictions and offences, including Personal data relating to criminal allegations and proceedings.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



Data controller: means the person or organisation that determines why, when and how Personal data is processed and is responsible for establishing practices and policies in line with Data Protection Laws. We are the Data controller of all Personal data relating to Data Users and Personal data used in our business for our own commercial purposes.

Data processor: means a natural or legal person, public authority, agency or other body which processes Personal data on our behalf and on our instructions, and which is not a Data User

Data subject: for the purpose of this policy, include all living, identified or identifiable individuals about whom we hold Personal data.

Data Users: are those of our colleagues (including temporary colleagues, agency workers, contractors, interns and volunteers) whose work involves processing Personal data. Data Users must protect the data they handle in accordance with this policy and any applicable data security procedures at all times.

Personal data: means any information identifying, or relating to, a Data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. It includes sensitive (special category) data, Criminal Convictions Data and pseudonymised Personal data but excludes anonymous data, or data that has had the identity of an individual permanently removed.

Processing: means any operation or set of operations which involves the use of Personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Sensitive (special category) personal data: is a special category of Personal data and includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic data, biometric data, health (including physical and mental health conditions), sex life or sexual orientation.

3. Data Protection Executive

The Data Protection Executive is responsible for ensuring our compliance with the Data Protection Laws and with this policy. If you have any questions or concerns about the operation of this policy, please contact the Data Protection Executive at dataprotection@marshalls.co.uk.

4. Data Protection Principles

4.1. All Data Users who process Personal data under this policy must comply (and be able to demonstrate compliance) with the principles of the Data Protection Laws. These principles provide that Personal data must:

4.1.1. be used in a way that makes it clear to Data subjects what is being done with their Personal data, and is fair, reasonable and compliant with Data Protection Laws;

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



- 4.1.2. only be used in line with how we told the Data subject we would use it and not for any wider, incompatible purposes;
- 4.1.3. be adequate, relevant and limited just to what we need it for;
- 4.1.4. be accurate and, where necessary, kept up to date;
- 4.1.5. not be kept in a form which permits identification of Data subjects for any longer than necessary for the purpose for which the Personal data is processed; and
- 4.1.6. be kept secure.

5. Fair and Lawful Processing

- 5.1. We must generally only process Personal data if there is a lawful basis to do so under Data Protection Legislation. This means that Marshalls will only process Personal data if one of the following applies:
 - 5.1.1. the Data subject has given us their consent (we must ensure that the consent wording and mechanism for obtaining consent meet the requirements of the Data Protection Laws);
 - 5.1.2. we need to process the Personal data to perform a contract with the Data subject, or because they have asked us to take certain steps before entering into a contract (for example, we may require contact details so we can process certain requests);
 - 5.1.3. the processing is necessary to comply with a legal obligation to which we are subject;
 - 5.1.4. the processing is necessary to protect someone's life or other vital interests;
 - 5.1.5. the processing is necessary to perform a task in the public interest; or
 - 5.1.6. the Processing is necessary for Marshalls' legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the Data subject's Personal data which overrides those interests.

6. Sensitive (Special Category) Personal Data, Criminal Convictions Data and Background Checks

- 6.1. Some of the information we hold as a business is particularly sensitive and special rules apply to it. Marshalls will only process Sensitive (special category) personal data and Criminal Convictions Data for the following purposes:
 - 6.1.1. to assess a colleague's fitness to work;
 - 6.1.2. to comply with health and safety obligations;
 - 6.1.3. to comply with the Equality Act 2010;

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland



- 6.1.4. checking applicants and colleague's right to work in the UK;
 - 6.1.5. verifying that candidates are suitable for employment or continued employment (i.e. criminal background checks); or
 - 6.1.6. for the recordings of CCTV images
- 6.2. The Data Protection Executive is responsible for monitoring Marshalls' use of Sensitive (special category) data and Criminal Convictions Data. Data Users must consult with the Data Protection Executive before using Sensitive (special category) data and/or Criminal Convictions Data to ensure the correct compliance steps are taken.

7. Processing for Limited Purposes

- 7.1. Personal data may only be processed for the specific purposes notified to the Data subject when the data was first collected or for any other purposes specifically permitted by law.
- 7.2. This means, broadly, that Personal data must not be collected for one purpose and then used for another without the Data subject being informed that their Personal data will be used for a new purpose. If it becomes necessary to change the purpose for which Personal data is processed, steps will need to be taken to inform the Data subject of the new purpose before any Processing occurs.

8. Notifying Data Subjects

- 8.1. To satisfy the transparency requirements under the Data Protection Laws, when collecting Personal data directly from Data subjects, Marshalls needs to ensure that the Data subjects receive fair information about how Marshalls will use their data.
- 8.2. Marshalls will provide them with the following information:
 - 8.2.1. our name and the contact details of the Data Protection Executive;
 - 8.2.2. the types of Personal data which we are collecting and Processing;
 - 8.2.3. why Marshalls is Processing their Personal data and the lawful basis that applies (for example, consent or legitimate interests);
 - 8.2.4. if Marshalls is Processing the Personal data on the basis of our, or a third party's, legitimate interests, Marshalls must explain what those interests are;
 - 8.2.5. anyone with whom Marshalls will share the Personal data (either their name or a general description of them) – this includes any suppliers to whom Marshalls may pass the data;
 - 8.2.6. details of transfers of the data outside the UK and safeguards Marshalls have put in place (such as binding corporate rules and standard contractual clauses approved for use in the UK);

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland



- 8.2.7. how long Marshalls plan to retain the Personal data or the criteria used to determine the retention period bearing in mind the Data Retention Policy;
 - 8.2.8. their legal rights as Data subjects (see paragraph 12 below);
 - 8.2.9. where we are Processing on the basis of consent, that they have the right to withdraw their consent at any time;
 - 8.2.10. their right to lodge a complaint with the ICO;
 - 8.2.11. whether the provision of Personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the data; and
 - 8.2.12. the existence of any automated decision-making, which produces legal effects concerning the Data subject or similarly affects the Data subject, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data subject.
- 8.3. If we receive Personal data about a Data subject from other sources, we shall provide the Data subject with the information outlined in paragraph 8.2 above, together with details of the categories of Personal data concerned and the source of the Personal data (and, if applicable, whether it came from a public source), as soon as possible thereafter.

9. Consent

- 9.1. Sometimes Marshalls will need consent to use a Data subject's Personal data. This is determined by the Data Protection Laws, and applies to areas such as direct marketing, unless another legal basis for processing applies (such as legitimate interests).
- 9.2. Where Processing by Marshalls is based on consent, we must be able to demonstrate that the Data subject has consented to Processing of their Personal data, and that the consent wording and mechanisms used for obtaining and recording consents are compliant with the Data Protection Laws.
- 9.3. Whenever we request consent for Processing, we will:
 - 9.3.1. present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;
 - 9.3.2. not use 'opt out' boxes or pre-ticked opt-in boxes;
 - 9.3.3. not make services conditional on consent to the Processing of Personal data that is not necessary for the performance of that contract (for example, marketing);
 - 9.3.4. keep records of consent obtained so we can provide evidence if required; and

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



- 9.3.5. enable Data subjects to withdraw their consent at any time.
- 9.4. A Data subject has the right to withdraw their consent to Processing at any time in accordance with their rights under Data Protection Laws. Data Users must consult with the Data Protection Executive if they receive a notification that a Data subject wishes to withdraw consent.
- 9.5. When assessing whether consent is freely given by the Data subject, utmost account shall be taken of whether, amongst other things, the performance of a contract, including the provision of a service, is conditional on consent to the Processing of Personal data that is not necessary for the performance of that contract.
- 9.6. When we process Sensitive (special category) personal data or Criminal Convictions Data, we will usually rely on a legal basis for processing (such as legitimate interests) other than consent if possible.
- 9.7. The Processing of children's Personal data may require additional parental consent. Data Users should consult the Data Protection Executive in relation to any Processing of children's Personal data to ensure that relevant compliance steps are addressed.

10. **Accurate Data**

We shall ensure that Personal data we hold is accurate and kept up to date. We shall check the accuracy of any Personal data at the point of collection and at regular intervals afterwards. We shall take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11. **Minimal Processing, Data Retention and Security Measures**

- 11.1. Marshalls will not collect excess Personal data or retain data for longer than we need it. This means:
 - 11.1.1. Marshalls will only collect Personal data to the extent that it is required for the specific purpose notified to the Data subject;
 - 11.1.2. Marshalls will not keep Personal data longer than is necessary for the purpose for which it was collected (except as required by law); and
 - 11.1.3. Marshalls will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, in line with the Data Retention Policy. For further information, please contact the Data Protection Executive.
- 11.2. We shall, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, in an effective manner and integrate the necessary safeguards into the
- 11.3. Processing in order to meet the requirements of the Data Protection Laws and protect the rights of Data subjects.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



11.4. We shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal data which is necessary for each specific purpose of the Processing is processed. That obligation applies to the amount of Personal data collected, the extent of its Processing, the period of its storage and its accessibility. In particular, such measures shall ensure that by default Personal data is not made accessible without the Data subject's intervention to an indefinite number of natural persons.

12. Processing in line with Data Subject's Rights

- 12.1. We shall process all Personal data in line with Data subjects' rights, in particular their right to:
- 12.1.1. be informed of how we process their Personal data;
 - 12.1.2. request access to any Personal data which we hold about them;
 - 12.1.3. ask to have inaccurate or incomplete Personal data amended;
 - 12.1.4. have Personal data erased from our systems (where such erasure is not prohibited by law);
 - 12.1.5. not to be subject to automated decisions (i.e. decisions made solely on a computer without human intervention) which produce legal effects or similarly significantly affect them, unless they have consented or another exception applies;
 - 12.1.6. a right to restrict, block or suppress our use of their Personal data and to prevent processing that is likely to cause damage or distress to themselves or anyone else;
 - 12.1.7. receive Personal data held about them in a commonly used, machine-readable format, and have the Personal data transmitted directly from one Data controller to another where it is technically feasible;
 - 12.1.8. object to us profiling them or sending targeted marketing to them; and
 - 12.1.9. where Processing of Personal data is based on consent (e.g. use of information for direct marketing purposes), a right to withdraw their consent at any time.

13. Data Security

- 13.1. Marshalls will ensure that appropriate measures are taken to keep Personal data secure. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss and Marshalls may incur large fines if Marshalls is in breach of the Data Protection Laws. You can also be criminally liable personally if you steal or recklessly misuse Personal data.
- 13.2. The Data Protection Laws require Marshalls to put in place procedures and technologies to maintain the security of all Personal data from the point of collection to the point of destruction.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



- 13.3. Marshalls will maintain data security by protecting the confidentiality, integrity and availability of the Personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the Personal data can access it.

Integrity means that Personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the Personal data if they need it for authorised purposes. Personal data must therefore be stored on the central computer system instead of individual desktops or devices.

- 13.4. Security procedures include:

Entry controls. Any unfamiliar person seen in entry-controlled areas should be reported.

Encryption. Any device that holds Personal data, including mobile devices and removable media, should be encrypted.

Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (Personal data is always considered confidential).

Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed or wiped when they are no longer required.

Equipment. Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their computer when it is left unattended.

- 13.5. Generally, to keep Personal data secure you must not disclose Personal data - in writing or verbally - to anyone not authorised to receive it, whether internal or external, and whether within or outside the workplace.

- 13.6. In addition to this policy, Data Users must comply with our Information Security Policy, together with our other IT policies accessible from Marshalls intranet which set out further information about how Marshalls keeps all data (including Personal data) secure.

14. Data Processors

- 14.1. We shall only use Data processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Data Protection Laws and ensure the protection of the rights of the Data subject.

- 14.2. Our contracts with Data processors shall set out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal data and categories of Data subjects and the obligations and rights of the Data controller.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



14.3. Our contracts with Data processors shall stipulate that the Data processor:

- 14.3.1. processes the Personal data only on our documented instructions;
- 14.3.2. ensures that persons authorised to process the Personal data are subject to appropriate confidentiality obligations;
- 14.3.3. takes all measures required to ensure the security of the Personal data;
- 14.3.4. shall not engage another Data processor without our prior written consent, and where another Data processor is engaged, it must be subject to obligations equal to obligations imposed on the original Data processor, and the original Data processor must remain fully liable to us for performance of its data protection obligations;
- 14.3.5. assists us by using appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of our obligation to respond to requests for exercising the Data subject's rights;
- 14.3.6. assists us to comply with our obligations under the Data Protection Laws;
- 14.3.7. shall, at our discretion, delete or return Personal data at the end of the service provision (unless required by law to store the Personal data);
- 14.3.8. makes available to us all information necessary to demonstrate its compliance with its data protection obligations in its contract with us; and
- 14.3.9. shall keep a written record (which may be in electronic form) of all Processing activities, which it shall make available to a supervisory authority on request, containing the following information:
 - 14.3.9.1. the name and contact details of the Data processor or processors and of each Data controller on behalf of which the Data processor is acting, and, where applicable, of the Data controller's or the Data processor's representative, and the data protection officer;
 - 14.3.9.2. the categories of Processing carried out;
 - 14.3.9.3. where applicable, transfers of Personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if applicable, the documentation of appropriate safeguards; and
 - 14.3.9.4. where possible, a general description of the technical and organisational security measures which are in place to protect Personal data.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



15. Transferring Personal Data to a Country Outside the UK

- 15.1. We may transfer any Personal data we hold to countries outside the UK, provided that one of the following conditions applies:
- 15.1.1. the UK has issued regulations confirming that the country to which we transfer the Personal data ensures an adequate level of protection for the Data subjects' rights and freedoms;
 - 15.1.2. the Data subject has given explicit consent to the proposed transfer;
 - 15.1.3. appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK;
 - 15.1.4. the transfer is necessary for one of the reasons set out in the Data Protection Laws, including the performance of a contract between us and the Data subject, to protect the vital interests of the Data subject;
 - 15.1.5. the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;
 - 15.1.6. in some limited cases, for our legitimate interests; and
 - 15.1.7. the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.
- 15.2. Subject to the requirements in paragraph 15.1 above, Personal data we hold may also be processed by colleagues operating outside the UK who work for us or for one of our suppliers. Such colleagues may be engaged in, among other things, the fulfilment of contracts with the Data subject, the Processing of payment details and the provision of support services.

16. Disclosure and Sharing of Personal Data

- 16.1. We may from time to time share Personal data with:
- 16.1.1. any member of our Group, which means our subsidiaries, our parent company, and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006;
 - 16.1.2. the Information Commissioner's Office (or any other relevant data protection regulatory authority);
 - 16.1.3. external providers, such as pension, insurance, reward and employee benefits providers or administrators;

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

12/2025 – Issue 8

Marshalls



- 16.1.4. in the event that Marshalls, its business, or substantially all of its assets are acquired by a third party (in which case Personal data may form part of the transferred assets); or
 - 16.1.5. in order to comply with legal obligations, or in order to enforce or apply a contract with an individual or other agreement; or to protect our rights, property, or safety of our colleagues, customers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- 16.2. We may share Personal data with Data processors in accordance with the terms of this policy.
- 16.3. The Data Protection Executive must be notified in advance in case a data sharing agreement needs to be entered into with the third party in order to help ensure that the sharing is compliant with Data Protection Laws.
- 17. Dealing with Subject Access Requests**
- 17.1. Data subjects may make a formal request for Personal data we hold about them. This must be made in writing. Colleagues who receive a written request should forward it to the Data Protection Executive immediately for guidance.
 - 17.2. When receiving telephone enquiries, we shall only disclose Personal data we hold on our systems if we verify the caller's identity to make sure that it is only given to a person who is entitled to it. If we are not sure about the caller's identity and where their identity cannot be checked; we shall suggest that the caller put their request in writing.
 - 17.3. Data Users shall refer a request to the Data Protection Executive for assistance in difficult situations. Data Users should not be bullied into disclosing Personal data.
 - 17.4. Where the request for Personal data is made in electronic form, we shall provide the information in electronic form where possible, unless otherwise requested by the Data subject.
 - 17.5. We shall deal with requests for information without undue delay. Within one month of a request for information, we shall either:
 - 17.5.1. provide the information to the Data subject;
 - 17.5.2. if the complexity or number of requests requires, extend the response period by up to a further two months and inform the Data subject of such extension; or,
 - 17.5.3. not action the information request and inform the Data subject of the reason for not taking action and of the possibility for lodging a complaint or seeking a judicial remedy.
 - 17.6. If requests for information are manifestly unfounded or excessive (particularly if they are repetitive), we may charge a reasonable fee to carry out the request or refuse to action the request. Employees who suspect they have received such requests should refer them to the

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

Data Protection Policy



Data Protection Executive. Otherwise, initial requests shall be dealt with free of charge, and we may charge a reasonable fee for further requests.

- 17.7 For further information on dealing with subject access requests please see the Data Subject Access Request Flow Chart on the Marshalls intranet, or contact the Data Protection Executive for guidance at dataprotection@marshalls.co.uk.

18. Data Protection Impact Assessments

- 18.1. Data Protection Laws require us to carry out a data protection impact assessment (“**DPIA**”) where our Processing activities are likely to result in a high risk of harm to a Data subject’s rights and freedoms.
- 18.2. As a general rule, the following activities will require a DPIA:
- 18.2.1. use of new technologies, or changes to existing technologies;
 - 18.2.2. the use of automated decision making and/or profiling;
 - 18.2.3. large scale Processing of Sensitive (special category) personal data or Criminal Convictions Data; and
 - 18.2.4. large scale, systematic monitoring of a publicly accessible area.
- 18.3 If any of these circumstances apply, please refer to the DPIA form on the Marshalls intranet, and contact the Data Protection Executive for guidance at dataprotection@marshalls.co.uk.

19. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we shall notify Data Users of this policy of those changes via the Marshalls intranet.

Approved and adopted by the Board of Marshalls plc on 4 December 2025.

Simon Bourne – Interim Chief Executive Officer

This policy will be reviewed annually.

For further information:

Marshalls plc – Group Legal and Company Secretarial Team
Landscape House, Elland

12/2025 – Issue 8

Marshalls