Issued: October 2022

Dunelm Group plc

Group Data Privacy and Protection Policy

Our customers, colleagues and all other individuals and businesses who engage with us trust Dunelm to keep their personal information safe, and to use it fairly and properly.

1. Commitment

Dunelm is committed to conducting its business in accordance with the UK's Data Protection Act 2018 (DPA) and all applicable data protection and privacy regulations.

We also require all third parties with whom personal data may be shared to make this commitment.

2. Policy and scope

This policy sets out the minimum standards that must be met by Dunelm Group plc and all subsidiaries ('Dunelm' or 'the Group') in relation to the collection, use, retention, transfer, disclosure and destruction of personal data. Dunelm is fully committed to ensuring the continued and effective implementation of the policy, and expects all colleagues to share in this commitment.

Non-compliance with this policy is taken seriously by Dunelm as it may expose us to complaints, regulatory action, fines and reputational damage. Any breach of this policy by a colleague may result in disciplinary action, up to and including dismissal.

Failure by a third party with whom we share personal data to adhere to applicable data protection and privacy regulations or related contractual commitments to us may lead us to seek redress or terminate our relationship with them.

3. Governance

Data protection responsibilities

The Board of Dunelm Group plc ('Group Board') is responsible for setting this policy, ensuring that appropriate processes are in place to ensure that it is complied with and for monitoring compliance.

The Executive Board is responsible for ensuring compliance with the UK's Data Protection Act 2018 and all applicable data protection legislation, the terms of this policy and that the processes to ensure compliance with this policy are operating effectively.

The Company Secretary is the appointed Data Protection Officer and accountable for legal and regulatory compliance, including compliance with the DPA.

The Chief Information Officer is responsible for the security and integrity of the IT systems across the Group.

Policy dissemination
The Executive Board must ensure that all Dunelm colleagues responsible for the processing of personal data are aware of and comply with this policy.

Compliance monitoring
The Head of Information Security will carry out an annual data protection compliance audit for key Dunelm functions.

A set of performance measures (KPIs) has been set to monitor compliance with key aspects of this policy. These are presented to the Risk and Resilience Committee monthly, and any failures to meet the KPIs are reported to the Executive Board and to the Audit and Risk Committee of the Dunelm Group Board.

,

4. Data protection principles
Dunelm colleagues must apply the following principles in the collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, fairness and transparency
Personal data will be processed lawfully, fairly and in a transparent manner. Dunelm must tell the person whose data is being processed (the data subject) what processing will occur (transparency); the processing must match the description given to the data subject (fairness); and it must be for one of the purposes specified in the DPA (lawfulness).

Principle 2: Purpose limitation
Personal data will be collected for specified, explicit and legitimate purposes and Processed only for those purposes. Dunelm must specify what the personal data collected will be used for, and this must fall within one of the DPA lawful purposes. The data can only be used to the extent necessary to fulfil the specified purpose.

Principle 3: Data minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Dunelm must not store any more personal data than strictly required for the purpose.

Principle 4: Accuracy
Personal data shall be accurate and kept up to date. Dunelm must have in place processes for correcting and/or deleting out-of-date, incorrect and redundant personal data.

Principle 5: Storage limitation
Personal data shall be retained no longer than is necessary for the purposes for which the personal data is processed. Dunelm must remove personal data when it is no longer required or store it in a way that prevents identification of the

data subject.

Principle 6: Integrity and confidentiality
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Dunelm must ensure that we have appropriate technical and organisational measures in place to keep personal data safe. Personal data should not be transferred to any third party or third country without appropriate safeguards being in place.

Dunelm must be able to demonstrate that the six Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

The application of these Data Protection Principles and the other terms of this policy must also be addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes which involve the processing of personal data, including entering into or renewing contracts with third parties. Examples of these may include (but are not limited to):

- IT contracts which relate to systems in which personal data is stored;
- Appointing a third party to analyse customer data;
- Sub-contracting activities which involve the personal data of colleagues or customers;
- Direct marketing activities;
- Appointing a new benefits provider.

5. External privacy notices

Each external website provided by Dunelm will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of the DPA and applicable law. These can be found here:

Customer website: dunelm.com

- Privacy policy: https://www.dunelm.com/info/help/privacy
- Cookie policy: https://www.dunelm.com/info/help/cookies

Corporate website: corporate.dunelm.com

- Privacy policy: https://corporate.dunelm.com/site-essentials/privacy-policy/
- Cookie policy: https://corporate.dunelm.com/media/2480/cookies-policy.pdf
- Shareholder privacy notice: https://corporate.dunelm.com/media/3138/shareholder-privacy-notice.pdf

Careers website: dunelmcareers.com

- Privacy policy: https://www.dunelmcareers.com/privacy-policy.aspx
- Cookie policy: https://www.dunelmcareers.com/cookie-policy.aspx

All Privacy and Cookie Notices must be approved by the Data Protection Officer and/or the Company Secretary or a member of her team prior to publication.

We are committed to updating any changes to our online 'Privacy Notice', online 'Cookie Notice' and this policy in a timely manner

5. Data security

Our security measures

Dunelm employs physical, technical, and organisational measures to ensure the security of personal data, in line with relevant industry guidelines. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted is set out in Dunelm Information Security Policies and outlined below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified or removed from a data processing system.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data is not kept longer than necessary.
- Ensure that personal data is encrypted whilst in transit and at rest.

Monitoring our information security systems

We are committed to risk-assessing, monitoring and, where necessary, upgrading our security systems on a regular basis and this is a Board and Audit and Risk Committee agenda matter, as detailed below.

Cyber and data security remains one of the most important risk areas to the Board and the Group as set out in the 'Principal Risks and Uncertainties' section in our recent Annual Reports, where we also formally report each year on our approach . We have a dedicated Information Security and Development Security and Operations team and data and information security issues are a standing agenda item for our Board Audit and Risk Committee.

We carry out regular data security testing of our systems, for example, formal penetration testing of high risk assets at least once a year.. Vulnerability assessments are carried out continuously. We carry out internal "phishing" tests, and colleagues who fail are required to complete additional training. We also assess the information security of all third parties to whom we transfer personal data before we start to do business with them.

We have a security incident management process that is tested at least once each year, a crisis management plan that would come into play in the event of any significant data breach and we have a legal obligation to notify the Information Commissioner and any individuals impacted of any major information security breach.

6. Data protection training
All Dunelm colleagues who have access to personal data will have their responsibilities under this policy outlined to them as part of their induction training and there is an annual refresher. In addition, regular data protection training and procedural guidance will be provided through Dunelm's online learning and development platform.

7. Complaints handling
Any complaint received from a data subject about the processing of their personal data is sent to Data Protection Officer (or team member). An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. We track all substantiated complaints through to resolution. The Company Secretary (or team member) will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

8. Data breach reporting
In the event of any notifiable data breach we are committed to contacting affected data subjects in a timely manner in accordance with our legal and regulatory obligations.

Any colleague who suspects that a personal data security incident has occurred must report the incident immediately via the Tech Service Desk. All reported incidents will be investigated in accordance with the Security Incident Response Process.

If required, the relevant Data Protection Authority (Information Commissioner's Office) and data subjects will be notified. We also commit to reporting the number of notifiable data breaches in the year in our annual report and accounts and/or ESG data sheet, available on our corporate website here:
https://corporate.dunelm.com/investors/reports-and-presentations/
https://corporate.dunelm.com/about-us/policies-and-statements/

Nick Wilkinson
CEO
October 2022