



Version: 2.0

Effective from September 2026

Code of Conduct for Goods not for Resale Suppliers



About this code

This Supplier Code of Conduct ('Code') establishes the minimum standards and behaviours that must be met by any entity that supplies goods or services to ASOS that are not for resale.

Corporate integrity, responsible sourcing, environmental sustainability and the safety and wellbeing of workers in the countries where we do business are of paramount importance to ASOS. All suppliers providing goods or services not for resale to ASOS must conduct themselves in line with these fundamental values.



Key definitions and scope

In this Code:

- **'Supplier'** means a body corporate, partnership or individual that provides goods or services that are not for resale to ASOS or one or more members of the ASOS group of companies.

Full definitions of technical terms used throughout this document are provided in [Appendix B](#).

The Code applies to Suppliers and throughout the whole supply chain, including sub-suppliers and subcontractors to Suppliers.

The Supplier shall comply with the Code and shall ensure that its workers and approved subcontractors act in compliance with the Code.

Core requirements of the Code

It is the Supplier's responsibility to ensure that the provision of all services is carried out in compliance with this Code.

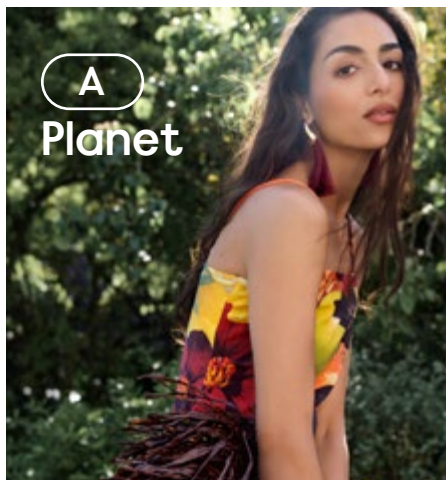
Suppliers must meet these core requirements in full and demonstrate ongoing compliance. Suppliers must ensure they have appropriate governance, management, stakeholder engagement, risk assessment and due diligence processes in place to ensure compliance.

ASOS will review and update this Code as required. It is the Supplier's responsibility to review any updates to the Code and take any action required to meet new or updated requirements, and to ensure its workers and approved subcontractors continue to comply with the Code.

Suppliers can contact ASOS with any queries using any of the contact details provided in [Appendix A](#).

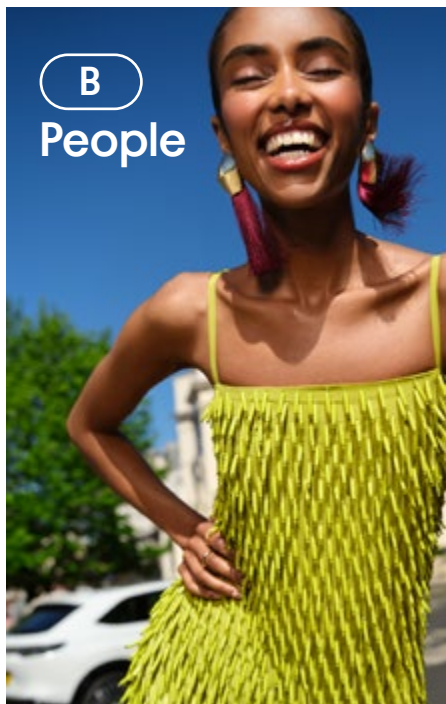


Core requirements of the Code



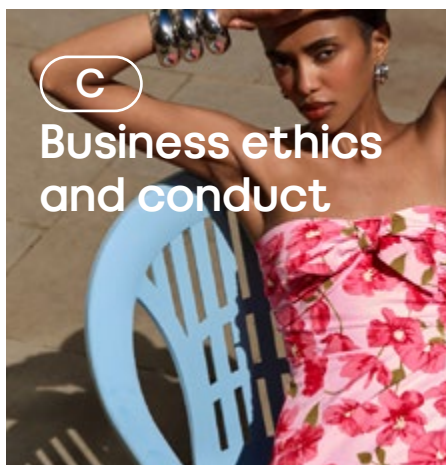
A Planet

- A1 Environmental management systems:** Suppliers must have policies and procedures in place to ensure compliance with environmental laws and regulations.
- A2 Waste and resource management:** Suppliers must ensure safe disposal of waste in full compliance with applicable laws and regulations and hold all required waste permits.
- A3,A4 Water and wastewater:** Suppliers must manage water and wastewater in full compliance with applicable laws and regulations.
- A5 Air emissions:** Suppliers must comply with all applicable air-emissions laws and regulations, hold all required air-emissions permits and operate in compliance with all permit conditions.



B People

- B1 Due diligence:** Suppliers must implement effective human rights due diligence policies to ensure human rights risks are identified and impacts remediated.
- B2 Modern slavery:** Suppliers must ensure all forms of forced labour, human trafficking and exploitation are prohibited and prevented. All recruitment practices must be fair and transparent, and workers must not be charged recruitment fees or related costs.
- B3 Child labour and young workers:** Suppliers must take proactive measures to prevent child labour.
- B4 Workers' rights:** Suppliers must protect workers' rights by keeping hours within legal limits, ensuring fair pay and benefits, preventing unlawful deductions, and providing safe, hygienic working conditions across the supply chain.
- B5 Freedom of association:** Suppliers must not prevent or discriminate against workers who wish to associate or bargain collectively.
- B6 Discrimination and sexual harassment:** Suppliers must prevent discrimination and sexual harassment in all its forms.



C Business ethics and conduct

- C1 Legal compliance:** Suppliers must comply with all applicable laws and the most stringent applicable standards, including obtaining and maintaining all required permits.
- C2 Anti-bribery and corruption:** Suppliers must have zero tolerance for bribery, corruption or improper influence.
- C3 Financial integrity and sanctions compliance:** Suppliers must prevent financial crime, including money laundering, fraud and tax evasion, and comply with all applicable sanctions regimes.
- C4 Data protection, cyber security and responsible use of AI:** Suppliers must protect all personal and commercial data, maintain strong cyber security practices and use AI systems ethically, transparently and in line with applicable laws and regulations.



Supplier commitment

The Supplier agrees that it will:

- comply with the requirements in this Code;
- maintain appropriate systems, governance and controls to ensure ongoing compliance and demonstrate compliance when requested by ASOS;
- provide information, documentation, certifications and evidence reasonably requested by ASOS to verify compliance;
- cooperate with audits, inspections, assessments and investigations carried out by ASOS in relation to compliance with this Code; and
- report any actual or suspected breach of this Code to ASOS.Compliance@asos.com as soon as possible.

Where requested in writing by ASOS, the Supplier must provide written confirmation within 30 days that it has appropriate systems in place to monitor compliance with this Code and is able to comply with this Code for the duration of its relationship with ASOS.

The Supplier must not retaliate against or take disciplinary action against any worker who, in good faith, has reported breaches of this Code, raised concerns about questionable behaviour, or sought advice regarding the Code.

Where required in regulation, Suppliers must maintain a due diligence policy covering human rights and environmental issues, including scope, processes and responsibilities.





Compliance, monitoring and remediation

Suppliers must operate in full compliance with applicable laws and the requirements set out in this Code.

This includes:

- monitoring supply chain risks and implementing policies and procedures to identify, address and prevent those risks;
- ensuring that adverse impacts are addressed through appropriate and effective remediation;
- promptly providing ASOS with full and accurate information, records and documentation requested to verify compliance with this Code; and
- providing transparent, accurate and timely information to ASOS and other relevant stakeholders where required.
- maintaining visibility of where services supplied to ASOS are conducted.
- providing information requested by ASOS to verify compliance and risk management.





Breaches and enforcement

This Code is intended to set minimum standards and support responsible supply chain management. ASOS values its partnerships with Suppliers and is committed to working with them to address issues, including where this Code is breached.

Suppliers must notify ASOS in writing of any actual or suspected material breach within 48 hours of becoming aware. The initial notification should include a brief description of the issue and any immediate actions taken. The Supplier must then actively cooperate with ASOS, including by providing evidence of the investigation approach and any remediation plan within one week of the initial notification.

ASOS reserves the right, at its sole discretion, to take appropriate operational, commercial and financial actions where a Supplier fails to meet the requirements of this Code, including where non-compliance, lack of evidence or non-disclosure creates risk for ASOS.

If ASOS becomes aware of a breach or alleged breach of this Code, ASOS may rely on any remedies available to it, including those set out in the relevant Supplier Agreement, and may terminate the Supplier Agreement where permitted.

Actions following a breach may be applied in conjunction with, or prior to, remediation or termination and may include, but are not limited to:

- Suspension of trading with the Supplier.
- Requiring the completion of corrective actions prior to the continuation of business.
- Holding the Supplier financially liable for all associated costs incurred by ASOS, including (but not limited to) detention, storage, re-routing, recall, loss of sale of stock, particularly where non-compliance, lack of evidence, or non-disclosure has contributed to the impact.
- Limiting further business growth or commercial opportunity.
- Requiring the Supplier to undergo a full re-assessment of compliance with this Code, including the application of enhanced due diligence, stricter evidence requirements and increased monitoring.

Where ASOS becomes aware that a Representative has been involved in an incident (or incidents) that would constitute a breach of any requirements under this Code, ASOS may either:

- (a) terminate its business relationship with the Supplier, including any contracts; or
- (b) require the Supplier to address the incident (or incidents) with the Representative.



If the Supplier is unable to resolve the issue with the Representative within a reasonable timeframe, ASOS may immediately terminate its business relationship with the Supplier, including any contracts.

ASOS may, at its discretion, provide the Supplier and Representative with support and resources to assist with remediation. Additionally, ASOS may suspend the business relationship with the Supplier while remediation is ongoing.

ASOS reserves the right to conduct an audit or inspection of any premises used in the provision of services to ASOS, including premises used by the Supplier or other third parties within the Supplier's supply chain, where ASOS reasonably suspects or becomes aware of a breach or alleged breach of this Code.

The Supplier must provide or obtain information and access to premises and individuals as reasonably required to investigate any breach or alleged breach. Suppliers must attend and participate in good faith in all review meetings reasonably requested by ASOS, including where such meetings relate to an audit, inspection, breach of the Supplier Agreement or breach of this Code.

If ASOS believes that a Supplier has attempted to withhold or falsify information requested by an ASOS representative, this shall be considered a breach of this Code.





Planet

Detailed Requirements



A. Planet

A1. Environmental Management Systems

A1

- Suppliers must have policies and procedures in place to identify, manage and remediate environmental risks; regularly review compliance with all applicable environmental laws, regulations, and permits, and document the procedure and findings.

A2. Waste Management

A2

- Ensure safe disposal of waste in full compliance with applicable laws and regulations.
- Hold all required waste permits and operate in compliance with all permit conditions.

A3. Water Use

A3

- Comply with all applicable water abstraction laws and regulations, including limits, licensing requirements, and any restrictions on water withdrawal.
- Hold all required permits and operate in compliance with all permit conditions.

A4. Wastewater Discharge

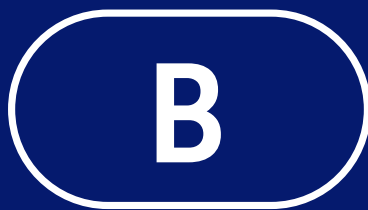
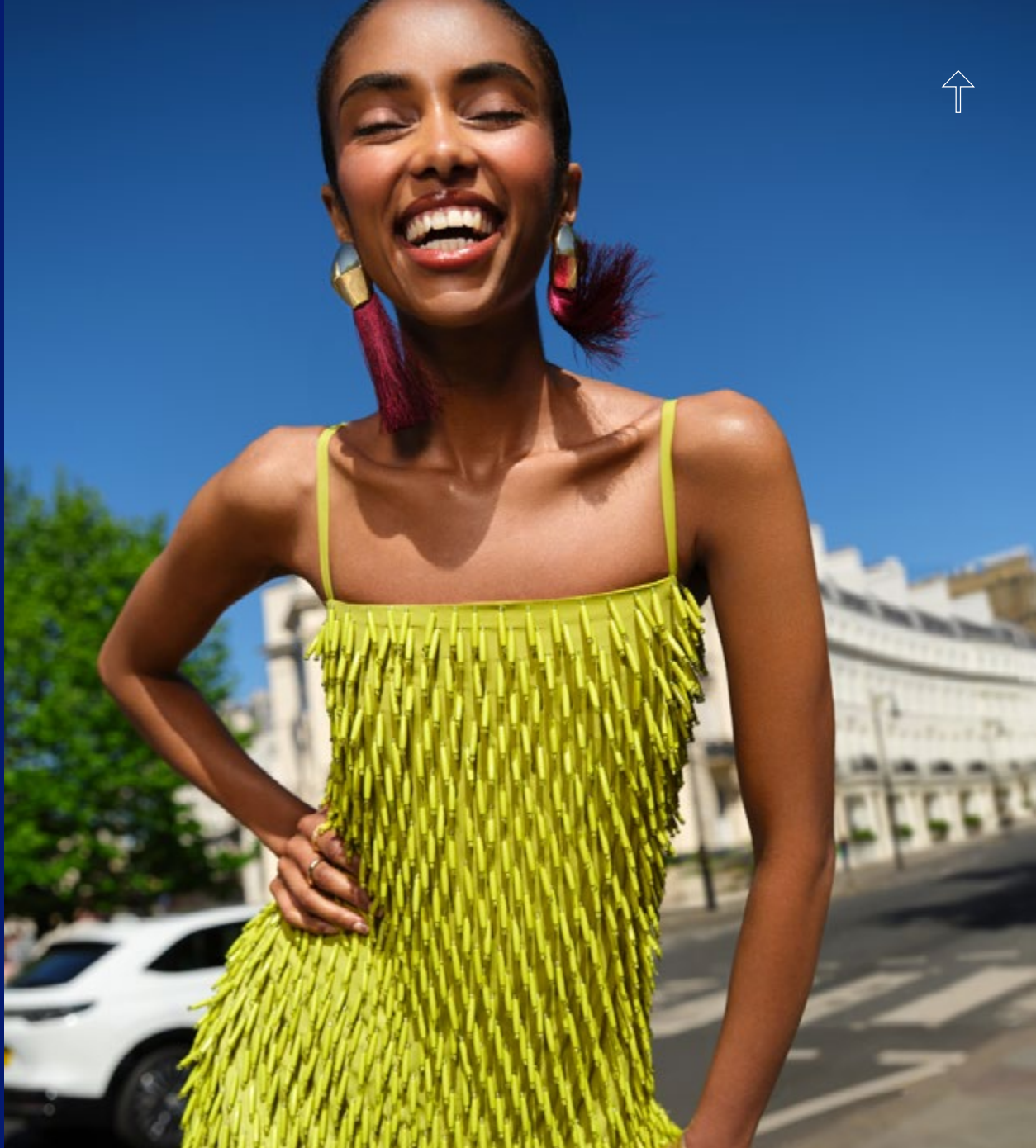
A4

- Manage wastewater in full compliance with applicable laws and regulations.

A5. Air Pollution

A5

- Comply with all applicable air emissions laws and regulations, including requirements to prevent uncontrolled or illegal releases of air pollutants.
- Hold all required air emissions permits and operate in compliance with all permit conditions.



People

Detailed Requirements



B. People

B1. Human rights due diligence

B1

- Monitor supply chain and implement policies and procedures which identify, address and prevent human rights risks and remediate impacts when necessary.
- Proactively declare to ASOS any human rights risks, allegations, or incidents and associated remediation.
- Respond to evidence requests from ASOS within required timelines.
- Engage in corrective actions as required by ASOS.

B2. Modern Slavery, Forced Labour and Human Trafficking

B2

- All forms of modern slavery are strictly prohibited throughout the supply chain, including forced labour, human trafficking, bonded labour, child labour, and state-imposed forced labour.
- Ensure that no services provided, sold or offered for sale to ASOS are linked in any way to forced labour. This includes indirect connections such as partnerships, group company links, or investment opportunities.
- Ensure the citizenship documents of workers, including workers of suppliers, are not withheld.
- All costs associated with employment eligibility and recruitment must be paid by the Supplier and must not be charged to or deducted from workers' wages. This includes recruitment fees, employment agency fees and any other associated recruitment costs.
- Ensure all workers have the right to enter and leave employment voluntarily, without any physical or monetary threats or barriers. Workers must not be subjected to any form of coercion or be forced to remain in their jobs against their will.
- Ensure workers are not coerced or physically confined to the workplace or provided accommodation. Workers must have the freedom to move and leave their place of work or accommodation without restrictions.
- Do not employ anyone below 15 years of age, or the local legal minimum age, or the age for completing compulsory education, whichever is higher. This is to ensure that children are not exploited and are protected from harmful work environments.
- Conduct thorough investigations of all allegations of modern slavery and implement corrective action plans. Cooperate with relevant authorities and partners to ensure victims have access to appropriate support.
- In the event that modern slavery occurs, develop and follow a remediation plan. This plan should be tailored to the specific details and root causes of the case.
- Remediation may include apologies, restitution, rehabilitation, financial or non-financial compensation, and punitive sanctions. The goal is to prevent further harm and ensure non-repetition.
- If a Supplier operates in the UK and the requirements under the Modern Slavery Act 2015 apply to its business, it must produce a modern slavery statement ('Statement') in accordance with [Government guidance](#).
- Suppliers must comply with any and all other applicable modern slavery reporting as required.



B. People

B3

B3. Child Labour Remediation and Young Workers

- Child labour is strictly prohibited and child workers must not be involved in the provision of services or goods not for resale to ASOS.
- Take proactive measures to prevent child labour by implementing rigorous age verification processes, monitoring compliance, and creating a safe working environment.

B4

B4. Workers' Rights, Wages, Benefits & Working Hours

- Ensure that workers throughout the supply chain are not obliged to work more than the regular workweek and maximum overtime set by local law and national or collective agreements.
- A regular workweek must not exceed 48 hours and one day off must be guaranteed for every seven-day period.
- Other than in exceptional circumstances, the sum of regular and overtime hours in a week must not exceed 60 hours.
- Overtime must be voluntary, compensated at a premium rate and not be requested on a regular basis.
- Suppliers and any other third parties within the Supplier's supply chain must pay at least the legal minimum wage in a timely manner, and all the legally mandated benefits including holidays and leaves, and statutory severance when employment ends.
- Disciplinary deductions from pay must not be made or tolerated.
- Suppliers and any other third parties within the Supplier's supply chain must adopt and adhere to rules and conditions of employment that respect workers, and, at a minimum, safeguard their rights under national and international labour and social security laws and regulations.
- All workers must have the right to refuse unsafe working conditions. Suppliers must provide a safe and hygienic working environment for all employees, with:
 - Systems in place to detect, avoid and respond to potential risks to the safety of all employees.
 - All possible precautions taken to prevent accidents at the workplace.
 - Manufacturing and storing buildings are safe and fire and emergency action plans are in place.
 - All safety measures in place at dorms, canteens, and childcare facilities.
 - Adequate personal protective equipment (PPE) must be provided. This must be provided free of charge and costs of PPE must not be deducted from pay.
- Take proactive measures to safeguard migrant worker rights and welfare, including by providing adequate training, ensuring fair treatment, and protecting their legal rights.
- Workers must have access to safe, confidential and anonymous channels to raise concerns, report misconduct or grievances, without fear of retaliation or adverse treatment.
- Adhere to all relevant laws and regulations.



B. People

B5. Freedom of Association and Collective Bargaining

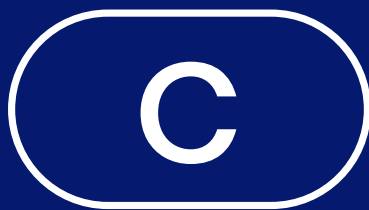
B5

- Do not prevent or discriminate against workers who wish to associate or bargain collectively.
- Where the right to freedom of association and collective bargaining is restricted under law, ensure suppliers allow for the development of parallel means for independent and free association and bargaining.

B6. Discrimination and sexual harassment

B6

- Do not permit discrimination in any form, including discrimination based on gender, sexual orientation, gender identity, marital status.
- Disciplinary deductions from pay must not be tolerated.
- Ensure everyone acting on the suppliers' behalf, including employees, agency workers, contractors, subcontractors and agents, treat ASOS employees with dignity, respect, and professionalism.
- Prohibited conduct can include, but is not limited to, unwanted physical or verbal conduct of a sexual nature, unwelcome sexual comments or jokes, or intrusive questions about someone's private life, regardless of intent. This can include interactions on ASOS, supplier, or other premises; during work trips or visits; or through telephone, email, messaging, or other digital communications.
- Assess and address the risks of sexual harassment and take appropriate preventative measures, including relevant training, safe working and visit arrangements, and clear reporting procedures. Promptly report concerns involving ASOS employees by emailing pxhub@asos.com or through our confidential external tool, Spot (talktopot.com/asos).



Business Ethics and Compliance

Detailed Requirements



C. Business Ethics and Compliance

C1

C1. General Compliance and Governance

- Operate in compliance with all applicable laws and regulations relevant to Supplier operations and the matters covered in this Code. To note:
 - Where there is a conflict between applicable laws, any agreement with ASOS, and this Code, the Supplier must comply with the most stringent standard.
 - Where there is a conflict between the provisions of an agreement with ASOS and the provisions of this Code, the Supplier must meet the more stringent standard.
- Maintain appropriate governance, controls, training, monitoring, record keeping and reporting processes to ensure compliance with the requirements set out in Section C of this Code, including in relation to third parties acting on the Supplier's behalf.
- Assign accountable personnel for oversight of business ethics, financial crime, data protection, AI and cyber security compliance, and review the effectiveness of those controls at regular intervals.
- Implement a training programme to ensure workers understand and comply with the requirements of this Code, and maintain records of all training provided.
- Maintain accurate records and be prepared to provide evidence of compliance when requested by ASOS.
- Cooperate fully with audits, inspections, assessments and investigations carried out by ASOS in relation to compliance with this Code.
- Ensure that relevant third parties, including subcontractors, agents and service providers, comply with applicable legal and ethical requirements and that appropriate due diligence and oversight are in place.

C2

C2. Business Integrity

- Conduct business with integrity, honesty and transparency. Any form of bribery, corruption, unethical conduct or improper influence is strictly prohibited.
- Comply with all applicable anti-bribery and corruption laws, including the UK Bribery Act 2010 and the US Foreign Corrupt Practices Act, and maintain appropriate internal controls to prevent bribery and corruption.
- Do not, directly or indirectly, offer, give, receive or solicit bribes or any improper advantage in any form. This includes improper payments, facilitation payments, kickbacks, secret commissions, or the use of third parties to circumvent anti-bribery requirements.
- Ensure that any gifts, hospitality, entertainment, charitable donations and sponsorships offered to ASOS employees are reasonable, proportionate, and for legitimate business purposes only. Suppliers must maintain appropriate approval, recording and monitoring controls for such items and must not use them to obtain or attempt to obtain an improper business advantage.
- Disclose any actual or potential conflicts of interest that may affect the business relationship with ASOS, including personal, family or financial relationships that could improperly influence decision-making. Suppliers must maintain a process for identifying, recording, assessing and managing conflicts of interest, including where conflicts arise through third parties acting on the supplier's behalf.
- Provide clear and accessible channels for workers to report concerns confidentially and without fear of retaliation. Suppliers must actively encourage reporting in good faith, communicate reporting routes to workers, investigate concerns promptly, keep appropriate records, and protect whistleblowers from harassment, discrimination or disciplinary action.
- Any suspected violations may be reported to ASOS through the confidential whistleblowing channel [SPOT](#).



C. Business Ethics and Compliance

C3

C3. Financial Crime Compliance

- Prevent financial crime within operations and supply chains, including money laundering, terrorist financing, sanctions breaches, fraud, and the facilitation of tax evasion. Relevant legal frameworks may include, but are not limited to, the Proceeds of Crime Act 2002, the Terrorism Act 2000, the Criminal Finances Act 2017, the Economic Crime and Corporate Transparency Act 2023, and applicable sanctions regimes, including those imposed by the United Nations, the United States, the European Union, and the United Kingdom.
- Implement appropriate risk assessments, internal controls, policies and procedures to identify, assess, prevent and respond to financial crime risks. These systems must include robust internal controls, policies, and procedures designed to detect and prevent illicit financial activities.
- Conduct due diligence on relevant business partners, suppliers and third parties, including enhanced scrutiny where there is a higher risk of sanctions, money laundering, fraud or tax evasion facilitation.
- Anti-money laundering policies and procedures should be regularly reviewed and updated to address emerging threats, ensuring that ASOS's supply chain remains secure and compliant with global anti-money laundering standards.
- Screen relevant parties and transactions against applicable sanctions lists and ensure that no business is conducted with sanctioned countries, individuals or entities unless expressly authorised by the relevant authorities. Suppliers must also comply with applicable export control and trade restrictions where relevant and maintain controls to prevent circumvention through intermediaries or indirect routing.
- Maintain accurate, detailed and secure records relating to financial crime controls, due diligence, screening, investigations and decisions, and retain those records for an appropriate period.
- Promptly investigate suspicious or unusual transactions or conduct and report concerns through appropriate internal and external channels where required by law.
- Implement fraud prevention and detection controls that are proportionate to the nature of the supplier's business, including segregation of duties where appropriate, financial and transactional oversight, escalation routes for suspected fraud, and investigation and remediation procedures.
- Provide regular training to employees on financial crime risks and responsibilities, including anti-money laundering, sanctions compliance, fraud prevention and anti-facilitation of tax evasion requirements.
- Promote a culture of tax compliance and ethical behaviour, and do not participate in, or facilitate, tax evasion in any jurisdiction. Comply fully with all obligations in relation to all taxes due in all jurisdictions in which the Supplier operates.
- Suppliers must comply with applicable Corporate Criminal Offence requirements under the Criminal Finances Act 2017 where relevant, including the maintenance of reasonable prevention procedures designed to stop associated persons from criminally facilitating tax evasion. Suppliers must treat such risks seriously even where senior management was not aware of the underlying conduct, and must retain records of risk assessments, controls, training and investigations.



C. Business Ethics and Compliance

C4

C4. Digital Responsibility and Security

- Manage personal data, digital systems and AI technologies responsibly, securely and in compliance with applicable laws, regulations and recognised standards, including UK GDPR, EU GDPR and any applicable local data protection laws.
- Ensure that personal data is processed lawfully, fairly and transparently, and only for specified and legitimate purposes. Where acting as a processor on behalf of ASOS, process personal data strictly in accordance with ASOS's documented instructions and not for any independent purpose. Implement and maintain appropriate technical and organisational measures to protect personal data and systems from unauthorised access, loss, destruction, damage or misuse. Such measures should be aligned to recognised standards such as ISO 27001, NIST or equivalent frameworks.
- Establish and maintain effective incident response and breach management procedures. Suppliers must notify ASOS without undue delay and in any event promptly upon becoming aware of any actual or suspected personal data breach or security incident affecting ASOS data or systems. Suppliers must document all incidents, including facts, effects and remedial action taken, and maintain a breach register in line with applicable legal requirements.
- Apply the principle of data minimisation and ensure that only personal data necessary for the relevant purpose is collected, accessed and retained. Suppliers must provide clear and transparent information regarding the collection, use and sharing of personal data.
- Respect individuals' rights in relation to their personal data and ensure appropriate processes are in place to identify, receive and respond to data subject requests within applicable legal timeframes.
- Maintain appropriate controls over data retention, deletion and access, including role-based access controls, regular access reviews and secure disposal of data when no longer required.
- Use AI technologies ethically and responsibly. AI systems must be transparent, accountable, designed to mitigate bias and discrimination, and implemented in a manner that respects privacy, security and human rights. Suppliers must also take account of applicable AI laws and regulations, including the EU AI Act where relevant. Suppliers must ensure appropriate human oversight, testing, validation, governance and record keeping before and during deployment of AI systems used in connection with ASOS business.
- Maintain strong cyber security practices, including access controls, multi-factor authentication where appropriate, monitoring, logging, regular review of access rights, vulnerability management, patching, backup and recovery arrangements, and ongoing cyber security training, in line with applicable cyber security laws and recognised standards.
- Ensure that any third parties, subcontractors or service providers that process personal data, use AI tools, or access systems on the Supplier's behalf are subject to appropriate due diligence, written agreements (including data processing agreements where required), and ongoing oversight to ensure compliance with applicable data protection, AI and cyber security requirements.
- Maintain appropriate records, policies and evidence to demonstrate compliance with the requirements set out in this section and provide such evidence to ASOS upon reasonable request.



Appendix A: Key Contacts

Topic	Key Contact
Compliance Matters	asos.compliance@asos.com
Business Ethics	asos.compliance@asos.com
Fraud	asos.compliance@asos.com
Cyber Security & Data Protection	DataProtection@asos.com



Appendix B. Definitions

Section A: Planet

- **Environmental Management System (EMS):** A structured framework that helps suppliers monitor and manage their environmental impacts, including energy use, waste, water and related risks.
- **Remediation:** Action taken to address harm when it occurs and prevent recurrence.

Section B: People

- **Child Labour:** Any use of a Child Worker for work, including forced, indentured or trafficked labour, or any exposure of a Young Worker to Hazardous Work.
- **Child Worker:** Someone who has not reached their 15th birthday, or any higher age specified in local law for completing mandatory schooling or beginning legal employment, and is therefore not legally entitled to work.
- **Child(ren):** Anyone below 18 years old.
- **Debt Bondage or Bonded Labour:** The use of debt as a mechanism of control over a person, forcing them to work to pay off the debt and losing control over the conditions of both their employment and the debt.
- **Discrimination:** Unequal treatment not permitted by law or ASOS policy, including treatment based on protected or personal characteristics, employment status or work status.
- **Forced Labour:** Work or service exacted from any person under threat of penalty and for which the person has not offered themselves voluntarily.
- **Hazardous Work:** Work likely to harm the health, safety or morals of children, including work with chemicals, machinery or electrics; in confined spaces; at height or in extreme temperatures; exposed to dust, fumes or loud noise; lifting heavy loads; or working overtime or at night.
- **Young Worker:** A worker who is above the legal minimum working age but below 18 years old.
- **AI system:** A machine-based system that can generate outputs such as predictions, recommendations, decisions or content for explicit or implicit objectives.
- **Financial crime:** Illegal or improper activity involving money or financial systems, including money laundering, terrorist financing, fraud, tax evasion facilitation and sanctions breaches.
- **Personal Data:** Information relating to an identified or identifiable individual.
- **Sanctions:** Legal restrictions imposed by governments or international bodies that limit dealings with specified countries, individuals, entities, goods, services or activities.

Section C: Business Ethics and Compliance

- **Access Control:** Measures to restrict access to information systems based on user roles and permissions.
- **Anti-Money Laundering (AML):** Measures and regulations designed to prevent the illegal generation of income through money laundering.
- **Associated persons:** An associated person can be any person who performs services for, or on behalf of the company. Some of the most common associated persons are employees, agents, contractors and third party service providers acting for or on behalf of the business.
- **Bribery:** Offering, giving, receiving, or soliciting something of value to influence a business decision.



Appendix B. Definitions

- **Conflicts of Interest:** Situations where personal or financial interests could potentially conflict with obligations to ASOS.
- **Corporate Criminal Offence (CCO):** Corporate Criminal Offences are set out in UK legislation. The Criminal Finances Act (2017) gives the UK government powers to recover any financial proceeds of crime, tackle money laundering, tax evasion and corruption and combat the financing of terrorism. The CCO rules make a business criminally liable if it fails to prevent its employees or other associated persons from helping someone evade tax. A business commits a CCO if all three stages occur:
 - A taxpayer commits criminal tax evasion (UK or foreign tax)
 - An “associated person” criminally facilitates that evasion (e.g. employee, agent, contractor, intermediary)
 - The business failed to prevent that facilitation
- A business may commit a CCO offence regardless of whether senior management or the Board were aware of the underlying conduct. A conviction can result in unlimited financial penalties, significant reputational damage and serious regulatory and commercial consequences.
- **Corruption:** Dishonest or fraudulent conduct by those in power, typically involving bribery.
- **Counter-Terrorist Financing:** Laws and regulations aimed at preventing the financing of terrorist activities.
- **Cybersecurity Laws:** Legal frameworks designed to protect information systems and data from cyber threats.
- **Data Minimisation:** The principle of collecting and processing only the personal data that is strictly necessary for the specified business purposes.
- **Data Privacy:** Measures taken to protect the privacy of individuals whose data is used in AI systems.
- **Data Security:** Measures taken to protect personal data from unauthorized access, loss, or damage.
- **Ethical AI Use:** The practice of using AI technologies in a manner that prevents harm and promotes transparency and accountability.
- **European Union AI Act:** Legislation aimed at regulating AI technologies to ensure they are used ethically and responsibly.
- **Fraud Prevention:** Measures and controls implemented to detect, prevent, and respond to fraudulent activities.
- **General Data Protection Regulation (GDPR):** A regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.
- **Gifts, Hospitality, Entertainment, Charitable Donations, and Sponsorships:** Items or services offered to ASOS employees that must be reasonable, proportionate, and for legitimate business purposes.
- **Incident Response Plan:** A strategy for detecting, mitigating, and remediating cybersecurity incidents.
- **Internal Controls:** Processes and procedures designed to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.
- **Monitoring and Compliance:** ASOS’s right to audit and assess suppliers’ compliance with Anti-Bribery and Corruption legal requirements and policies.
- **Multi-Factor Authentication:** Security process requiring multiple forms of verification to access systems.
- **Proceeds of Crime Act 2002 (UK):** Legislation that addresses the recovery of assets obtained through criminal activities.
- **Prohibition of Bribery and Corruption:** ASOS’s zero-tolerance policy towards bribery and corruption, prohibiting the offering, giving, receiving, or soliciting of bribes or improper advantages in any form.
- **Reporting and Whistleblowing:** Mechanisms to detect and prevent bribery and corruption, and channels for reporting suspected violations.
- **Tax evasion:** Tax evasion is the deliberate and dishonest act of not paying tax that is legally due, by concealing income, assets or information, or by providing false or misleading information to tax authorities. It is illegal and a criminal offence.
- **Terrorism Act 2000 (UK):** Legislation that provides the legal framework for counter-terrorism measures in the UK.
- **Whistleblowing:** Reporting concerns about wrongdoing, unethical behaviour, or violations of policies in a confidential manner.