Code of Ethics

In circumstances of any material breaches to AAG's Code of Ethics Policies, the following may apply:
- Breaches, including case details, may be reported to the Board of Directors
- Reported breaches will be investigated promptly via independent 3rd party and may be reported publicly.
- Employees may face disciplinary actions, including dismissal.
- Contracts with business partners who are found in breach will be terminated.

Code of Ethics

As a member of the Active Apparel Group (AAG), you are expected to adhere to the following code of ethics:

1. **Honesty and Integrity:** We expect our employees to conduct themselves with honesty, integrity, and professionalism at all times. This includes being truthful in all communication, respecting the confidentiality of sensitive information, and avoiding any conflicts of interest.
2. **Respect:** We value diversity and respect for others' beliefs, opinions, and cultures. Employees must treat colleagues, customers, and stakeholders with respect, empathy, and fairness.
3. **Responsibility:** We take our responsibility seriously, and we expect our employees to take ownership of their actions and decisions. Employees should fulfill their duties with diligence, accountability, and excellence, and report any concerns or issues to appropriate channels.
4. **Compliance:** Our organization complies with all applicable laws, regulations, and ethical standards. Employees must comply with these rules, as well as our internal policies and procedures.
5. **Professional Development:** We encourage our employees to pursue ongoing learning and development to enhance their skills and knowledge. Employees should strive for continuous improvement and contribute to the growth and success of our organization.
6. **Social Responsibility:** We believe in giving back to our communities and the environment. Employees should consider the impact of our activities on the environment, society, and the economy, and act responsibly to promote sustainable development.
7. **Non-Discrimination:** We value diversity and oppose discrimination based on race, gender, age, religion, sexual orientation, nationality, or disability. Employees should promote a safe, inclusive, and respectful workplace that values diversity and fosters equality.

The code of Ethics also encompasses a number of core policies. These policies outline a series of important areas that each employee must read and understand.

These policies are:

- Anti-Bribery / Anti-Corruption
- Privacy
- Information Security
- Whistle-blower

Table of Contents

Anti-Bribery / Anti-Corruption Policy

Introduction

Bribery is the offering, promising, giving, accepting, or soliciting of an advantage as an inducement for action which is illegal or a breach of trust. A bribe is an inducement or reward offered, promised, or provided in order to gain any commercial, contractual, regulatory, or personal advantage.

Corruption refers to the abuse of power or position for personal gain or the gain of a particular group, often through illegal or unethical means. It can take many forms, including bribery, embezzlement, nepotism, fraud, and extortion. Corruption can occur in various contexts, such as in government, business, and politics, and it can have serious consequences for individuals, organizations, and society as a whole. Corruption undermines trust in institutions, distorts the allocation of resources, stifles economic growth, and undermines the rule of law.

It is a global problem that affects both developed and developing countries. It is our policy to conduct all of our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships by implementing and enforcing effective systems to counter bribery. We will uphold all laws relevant to countering bribery and corruption in each country that we have a presence – Australia, The United States of America and China.

Objective

The objective of creating an anti-bribery/anti-corruption policy is to establish guidelines and procedures that prevent and detect bribery and corruption within an organization. The policy aims to create a culture of integrity, transparency, and accountability by setting expectations for ethical conduct and establishing consequences for non-compliance.

Purpose

The purpose of this policy is to establish controls to ensure compliance with all applicable anti-bribery and corruption regulations, and to ensure that the Active Apparel Group's business is conducted in a socially responsible manner.
This policy forms part of the overall Code of Ethics/Conduct for the Active Apparel Group.

Scope

Who is covered by the policy?

In this policy, third party means any individual or organisation you come into contact with AAG during the course of their work for us, and includes actual and potential clients, vendors, contractors, business contacts, agents, and government and public bodies.
This policy applies to all employees and contractors engaged by AAG, collectively referred to as personnel.

This policy covers:

- Bribes
- Gifts and hospitality
- Charitable contributions
- Political contributions

a. Bribes

Personnel must not engage in any form of bribery, either directly or indirectly.

b. Gifts and hospitality

Personnel must not offer or give any gift or hospitality:

- which could be regarded as illegal or improper, or which violates the recipient's policies or
- to any public employee or government officials or representatives.

Employees may not accept any gift or hospitality from any business associates, vendors or contractors unless previously authorised by the Chief Executive Officer.

c. Charitable contributions

Charitable support and donations are acceptable (and indeed are encouraged), whether of knowledge, time, or direct financial contributions. However, personnel must be careful to ensure that charitable contributions are not used as a scheme to conceal bribery.

d. Political contributions

We recognize that political contributions should be made transparently and fully disclosed in accordance with all applicable laws and regulations. We will not make any political contributions in exchange for or in anticipation of any business or regulatory advantage.
AAG is committed to public disclosure of financial and in-kind contributions to political parties, politicians, lobby groups or advocacy groups.

Your responsibilities

You must ensure that you read, understand, and comply with this policy. The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for AAG.

All employees are required to avoid any activity that might lead to, or suggest, a breach of this policy. You must notify your manager as soon as possible if you believe or suspect that a conflict with or breach of this policy has occurred or may occur in the future.

Personnel who breach this policy will face disciplinary action, which could result in dismissal for gross misconduct.

We reserve our right to terminate our contractual relationship with other workers if they breach this policy.

Our responsibilities

AAG is committed to investigate all breaches and ensuring case details are reported to the Board of Directors, reported publicly, and investigated promptly by an independent party.

This policy will be reviewed and renewed annually based on the reported cases and other opportunities for improvement.

1. How to raise a concern

You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage.

If you are unsure whether a particular act constitutes bribery or corruption, or if you have any other queries or concerns, these should be raised with your manager. Please see the Whistle-blower policy for details on reporting your concerns.

2. What to do if you are a victim of bribery or corruption

It is important that you tell your manager as soon as possible if you are offered a bribe by a third party, or are asked to make one, suspect that this may happen in the future, or believe that you are a victim of another form of unlawful activity.

3. Protection

Personnel who refuse to accept or offer a bribe, or those who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions.

We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. (see the Whistle-blower companion policy)

We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place or may take place in the future.

4. Training and communication

Training on this policy forms part of the induction process for all new employees. All existing employees will receive relevant training on how to implement and adhere to this policy. In addition, all employees will be asked to formally accept conformance to this policy on an annual basis.
Our zero-tolerance approach to bribery and corruption must be communicated to all vendors, suppliers, contractors, and business partners at the outset of our business relationship with them and as appropriate thereafter.

5. Who is responsible for the policy?

The Board have overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all personnel comply with it.
The Chief Executive Officer has primary and day-to-day responsibility for implementing this policy, and for monitoring its use and effectiveness and dealing with any queries on its interpretation.

6. Monitoring and review

The Chief Executive Officer will monitor the effectiveness and review the implementation of this policy, regularly considering its suitability, adequacy, and effectiveness.
Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.
All personnel are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.
Personnel are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions, and queries should be addressed to the Chief Executive Officer.

7. Public disclosure

As a responsible organization, we believe in conducting business ethically and with integrity. Our Code of Ethics is designed to guide our actions and decisions in line with these principles. We recognize the importance of transparency and accountability in our operations and hereby declare the following:

1. **Compliance with Laws and Regulations:** We are committed to complying with all applicable laws, regulations, and industry standards. We will not engage in any activities that violate these laws, regulations, or standards.
2. **Ethical Conduct:** We expect all our employees and stakeholders to behave ethically and with integrity. We will not tolerate any behaviour that is unethical, dishonest, or illegal. We will encourage open communication and provide a safe and respectful working environment.

3. **Conflict of Interest:** We will avoid any situation that creates or appears to create a conflict of interest. We will disclose any potential or actual conflicts of interest and take appropriate measures to manage them.
4. **Protection of Confidential Information:** We will protect the confidential information of our organization, our customers, and our stakeholders. We will not disclose this information except as required by law or with the appropriate authorization.
5. **Fair Competition:** We will compete fairly and ethically in the marketplace. We will not engage in any activities that are anti-competitive, such as price-fixing or market manipulation.
6. **Social Responsibility:** We recognize our responsibility to society and the environment. We will conduct our business in a manner that respects the environment, human rights, and social responsibility.
7. **Reporting of Violations:** We encourage the reporting of any violations of our Code of Ethics. We will investigate all reported violations and take appropriate action.

This public disclosure statement is made to demonstrate our commitment to ethical behaviour and transparency. We will regularly review and update our Code of Ethics to ensure that it remains relevant and effective.

Privacy Policy

Version	Modification Date	Last Modified By	Document Changes
0.1	14/11/2022	Terence Wallis	Initial Draft of the Privacy policy
1.0	20/01/2023	Terence Wallis	Sent for review and approval
2.0	21/06/23	Hamilton Locke	Review and feedback
3.0	29/06/23	Terence Wallis	Updated – ready for board review & approval

Introduction

The Active Apparel Group (we, us or our) is committed to protecting the privacy of personal information that we hold. This Privacy Policy explains how we collect, use, disclose and hold personal information and how to contact us if you have any queries about personal information that we hold about you.

Personal Information

Under the Privacy Act 1988 (Cth), "Personal information" is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

The kinds of personal information we collect and hold

We collect and hold a range of personal information in carrying out our business and functions as a manufacturer and wholesale supplier of active wear and swimwear products. The kinds of personal information we collect and hold about you will depend upon the nature of our relationship with you and the circumstances of a collection, including whether we collect the information from you as a customer, supplier, contractor, job applicant or some other capacity.

For example:

- if you are a wholesale customer, we may collect your name, work address, telephone number and email address, and any other information you provide to us when you make an inquiry, request information, submit an order, provide feedback or correspond with us;
- if you are a job applicant, we may collect your name, address, telephone number, email address and employment history, and any other information you provide to us during the application and recruitment process; and
- if you deal with us in some other capacity, we may collect your name and contact details and any other information you choose to provide to us.

We may also collect details of the interactions you have with us.

We do not generally collect sensitive information and we will only collect sensitive information about you with your consent (unless we are otherwise required or authorised by or under law to do so).

How we collect personal information

We collect personal information in a variety of ways, including:

- from you directly (such as when you interact with us in writing, electronically or by telephone);
- when you communicate with us through our website;
- from third parties such as [insert e.g., business partners or sales representatives]; and
- from media, publications, and other publicly available sources.

When we obtain personal information from third parties to whom you refer us, we will assume and you must ensure that you have made that third party aware that you have referred us to them and of the purposes involved in the collection, use and disclosure of the relevant personal information.
If you provide us with personal information about another person, please make sure that you tell them about this Privacy Policy.
If you are or become an employee, the handling of your personal information may be exempt from the Australian Privacy Principles under the Privacy Act 1988 (Cth) if it is directly related to your current or former employment relationship with us.

The purposes for which we collect, hold, use and disclose personal information

We collect, hold, use and disclose personal information for a range of purposes including:

i. to supply our products and services (such as account creation and fulfilling and managing your orders, payments, returns, and exchanges made though our sites);
ii. to send you administrative information (such as product, service update and/or information about changes to our terms, conditions, and policies);
iii. to protect our sites (such as fraud monitoring and prevention);
iv. for our administrative purposes and internal record keeping;
v. to perform research and analysis and improve or develop our products or services;
vi. to manage our relationships with our customers, suppliers and contractors;
vii. to consider job applicants for current and future employment;
viii. where we believe it is necessary to investigate, prevent or act regarding potential violations of our policies, suspected fraud, situations involving personal threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved; and
ix. to comply with our legal and regulatory obligations.

We may use and disclose your personal information for other purposes required or authorised by or under law (including purposes for which you have provided your consent).

If we are unable to collect personal information from or about you, we may not be able to respond to your requests or enquiries in certain other dealings with you.

Disclosure of personal information to third parties

In conducting our business, we may disclose your personal information to third parties for the purposes outlined above. These third parties may include, where appropriate:

- our related companies (including our parent company and any subsidiaries, joint ventures partners or other companies that we control or that are under common control with us);
- financial institutions for payment processing;
- our contracted service providers, including:
    - delivery and shipping providers
    - IT service providers
    - marketing, promotional and market research agencies; and
    - external business advisers (such as auditors and lawyers);
- to other third parties in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another entity; and
- if you are a job applicant, referees whose details you provide to us.

We may also disclose your personal information to other third parties and for other purposes where we are required or authorised by or under law to do so (including where you have provided your consent).
We may allow selected third parties to use tracking technology on our sites, which will enable them to collect data about how you interact with these sites over time. Unless described in this policy, we do not share, sell, rent, or trade any of your information with third parties for their promotional purposes.

Cookies

We use data collection devices such as “cookies” on certain web pages to help analyse our web page flow and measure marketing effectiveness.
Cookies are used to create a session and remember your use of our website. This provides additional convenience for your visit to the site, including remembering account information, currency and location.
For this reason, it is necessary that you enable cookies in your browser, and you hereby acknowledge that we have informed you of our use of cookies and that you consent to our use of cookies in relation to your computer system.

Overseas disclosure of personal information

Some of our service providers and related companies are located outside Australia. As a result, personal information collected and held by us may be transferred to recipients in other countries. In particular, we may disclose personal information to our related companies located in China, Hong Kong and the USA. We may also use service providers located in a range of countries to store customer data, including in Hong Kong.

How we hold personal information

We generally hold personal information in computer systems, including computer systems operated for us by our service providers. We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure. This includes taking appropriate security measures to protect electronic materials and requiring our service providers to do so.

Access to and correction of your personal information

You have a right to request access to personal information that we hold about you and request its correction if it is inaccurate, out of date, incomplete, irrelevant, or misleading. You may do so by contacting us using the contact details at the end of this policy.

We will respond to all requests for access to or correction of personal information within a reasonable period.

We will generally provide you with access to your personal information (subject to some exceptions permitted by law) but may charge an access fee to cover the cost of retrieving the information and supplying it to you.

Complaints

Please contact us (using the contact details at the end of this policy) if you have any concerns or complaints about the manner in which we have collected or handled your personal information. We will inquire into your complaint and respond within 30 days. If you are not satisfied with our response, you can contact us to discuss your concerns or lodge a complaint with the Australian Information Commissioner (oaic.gov.au).

Notification of changes

From time to time it may be necessary for us to review and revise our Privacy Policy. We may notify you about changes to this Privacy Policy by posting an updated version on our website. We encourage you to check our website from time to time to ensure you are familiar with our latest Privacy Policy.

Our Privacy Policy was last updated in June 2023.

Contact Us

If you would like more information about the way we manage personal information, would like to request access to or correction of personal information that we hold about you, or wish to make a complaint, please contact us by either:

Email – info@activeapparel.com

Post – Level 2, 365 MacArthur Avenue, Hamilton, QLD, 4007

Telephone – +61 468 384 984

Information Security Policy

Version	Modification Date	Last Modified By	Document Changes
0.1	14/09/2022	Terence Wallis	Initial Draft of IS policy
0.2	15/09/2022	Terence Wallis	Updated the following sections – Acceptable use, Enforcement & Disciplinary Action
1.0	15/11/2022	Terence Wallis	Adding Companion Policy references to the IS Policy
2.0	20/01/2023	Terence Wallis	Sent for final review & approval
3.0	16/03/2023	Terence Wallis	Extensive input /changes made to the core document based on feedback from the Protiviti Cyber Security consultant.

Purpose

Effective protection of business information creates a competitive advantage, both in the ability to preserve the reputation of Active Apparel Group (AAG) and in reducing the risk of the occurrence of negative events and incidents.

The purpose of this information security policy is to:

a. Establish an organization wide approach to information security.
b. To detect and forestall the compromise of information security such as misuse of data, networks, computer systems, and applications.
c. To protect the reputation of the company with respect to its ethical and legal responsibilities.
d. To protect our employees and customers.

Scope

This Information Security policy provides the basis of Information Security management within AAG.

This policy applies to all AAG employees, contractors, vendors, third parties and anyone else who may have any type of access to AAG systems, software, or hardware.

Logical Security

a. Software Security

i. All users connected to the network are supplied with a User Account for authentication and allocation of appropriate access rights to network facilities including software. Access to such network facilities and

software is controlled using secure passwords which must be changed on a regular basis (see password security).

ii. All employee laptops must be set with an inactivity screensaver which requires a username and password to reactivate the underlying session.

iii. As a means of allocating appropriate software packages to specific users, the use of an application deployment tool will be used. This will grant individuals or groups access to various programs and services in accordance with their duties and requirements through their user account.

iv. By default, AAG supplied computing devices do not have administrator privileges, this is to prevent the unauthorised installation of software packages. Only IT support, with approved admin access can install applications or execute executables.

v. All endpoints used by employees to connect to the corporate network shall use IT managed devices, whereby the AAG IT controls settings and access.

vi. All contractors, vendors or suppliers accessing the AAG environment or data are required to adhere to the security policies.

vii. All access to the AAG environment from outside parties must meet the agreed standard information security policies.

b. Software Development

i. Software development and configuration must be performed in a controlled, test environment until such time that all critical and high bugs, flaws, and potential vulnerabilities are removed.

ii. Only solutions that have approval from the Change Advisory Board (CAB) may be promoted to a production environment.

iii. It is imperative that a rollback path and plan are in place prior to deployment into a production environment.

iv. All process steps must be completed by the team promoting the solution into production to ensure a timely and accurate deployment. These steps must be auditable via system logs with user credentials and timestamps identified.

v. Any software development that may cause harm or impact the employees of the Active Apparel in an adverse manner including, but not restricted to, scanning, gaining unauthorised access, exploiting vulnerabilities to take advantage of exploits, will be looked upon as

inappropriate and treated as a direct attempt to compromise the organization and thus treated appropriately (see Disciplinary Action).

c. Software as a Service (SaaS)

i. Software as a Service (SaaS) is the provision of software solutions provide and hosted by external providers in a Cloud environment accessed via the internet. Use of SaaS has many benefits but also requires significant consideration, investigation, and discussion prior to the use of such services for AAG activities.

ii. Governance and compliance are critical aspects in the success of introducing innovative solutions into the business. This includes clearly identified ownership across the following areas – application owner, business owner, data owner, technical owner.

iii. Prior to engaging and/or onboarding a new SaaS provider AAG will provide the Information Security policy along with other key documents that outline our SLA's and expectations of the supplier, or vendor.

iv. It is essential that the Business Transformation Office be included in all discussions when considering SaaS solutions to ensure that the service fits with the organizations technology architectural requirements and meets a set of standards around data, security, access, and any contracts between the AAG and the vendor.

v. No agreement will be entered into with a supplier or vendor without specific involvement of the Business Transformation Office as these services can expose the organization to an unacceptable level of risk. It is also possible that by entering into an agreement without Transformation Office involvement, you place the AAG in a tenuous legal position that may have wide ranging implications.

d. End-Point Security and Antivirus Software

i. All AAG owned laptops have end-point security software installed which is recommended by the vendor and that has an update feature enabled. This is to ensure that the software is kept updated for the latest threats. There are also email filtering systems in place checking all incoming email into the organisation and on internally circulating emails.

ii. All non AAG endpoints must meet the security standards including current updated antivirus software installed, and it is the owner's / user's responsibility to ensure this.

iii. Not having current updated antivirus software installed exposes our systems and infrastructure to potentially significant disruption and damage due to virus infected computers.

e. Password Requirements

Passwords for elevated accounts, privileged accounts and serve accounts should have unique and higher standards than normal users.

To avoid employees' work account passwords being compromised, these best practices are advised for setting up passwords:

i. Use at least 8 characters (must contain capital and lower-case letters, numbers, and symbols) – preferably not a word
ii. Do not write down passwords and/or leave it unprotected
iii. Do not exchange credentials when not requested or approved by supervisor/manager
iv. Change passwords every 90 days
v. Old passwords cannot be reused

f. Patch Management

i. To ensure that all operating systems and applications are kept current and up to date, a central Patch Management Server will be used. This server will send out any operating system and/or software updates, to all AAG laptops, that are required to address any known software vulnerabilities. These updates will be distributed at the discretion of the BTO.

ii. Only tested and approved patches via CAB will be deployed.

iii. Ongoing monitoring of our Patch management system will be performed. All patching activities will be

iv. Regular checks will be performed on all servers to assess their vulnerability status at any given time. This task will be managed by the AAG IT Service desk.

Data Security

1. Confidential Data Security

Confidential data security applies to all employees, contractors, vendors, and third parties who have access to AAG's confidential data.

i. **Access Controls:** Access to confidential data is limited to authorized personnel only. Access controls such as password protection, two-factor authentication, and physical security measures are implemented to

prevent unauthorized access. Employees are required to maintain the confidentiality of their login credentials and report any suspicious activity to their supervisor immediately.

ii. **Data Classification:** All data is classified according to its sensitivity level. Confidential data is identified, marked, and stored in a secure location. Data that is no longer required is disposed of securely.

iii. **Data Encryption:** All confidential data in transit and at rest is encrypted using industry-standard encryption algorithms.

iv. **Third-Party Access:** Third-party access to confidential data is granted on a need-to-know basis only. Third-party service providers are required to comply with [Company Name]'s data security policies and sign a confidentiality agreement before accessing any confidential data.

v. **Incident Response:** All suspected data breaches or security incidents must be reported immediately to the IT department. [Company Name] has a comprehensive incident response plan in place that includes investigation, containment, and notification procedures.

vi. **Training and Awareness:** All employees are required to undergo data security and privacy training to ensure they understand their responsibilities and comply with [Company Name]'s data security policies. Employees are also required to sign a confidentiality agreement acknowledging their understanding of their obligations.

vii. **Compliance:** AAG complies with all relevant data protection and privacy regulations, including but not limited to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Note: Failure to comply with this policy may result in disciplinary action, including termination of employment or termination of a contract. If you have any questions about this policy or any data security concerns, please contact the IT department.

Data Encryption

i. Data encryption is a method used to reduce the readability of data should it be accessed via unauthorised means by encrypting the data so that without the decryption key the data is undecipherable. This can include data stored on corporate production databases or information stored within our systems and devices.

ii. All data both in motion and rest within AAG's production databases must be encrypted using approved encryption methodologies including encryption key storage and management.

iii. Access to data should only be available via credential-controlled applications with limited exceptions to this process for BTO staff such as approved system and database administrators.

Data Breaches

i. Loss or theft of data is a serious matter and carries with it legislative compliance requirements and potential financial penalties for misuse or inappropriate distribution of certain data.

ii. A data breach can include, but is not limited to, unauthorised system access, loss or theft of storage or mobile / portable devices, inclusion of inappropriate data in existing data sets, email attachments sent to unauthorised or incorrect recipients or printed documents containing protected data accessible by unauthorised people.

iii. If a potential data breach is detected by anyone within the AAG, it is critical that the matter be reported to the Chief Transformation Officer immediately for investigation and follow-up.

Communication Security

i. Communications can take various forms which include, but are not restricted to, voice via land line, voice via mobile phone, voice via computer network (VOIP), email, electronic file transfer, wireless access, Virtual Private Network (VPN) connections, Infra-Red (RFID), Bluetooth and ITS network infrastructure.

ii. Each of these communications methods poses its own unique security problems and needs to be addressed individually. In each case, where network communications are required, irrespective of type, only those methods as permitted by BTO will be allowed and must be in accordance with the specific Communications Security procedures which are to be developed to support this policy.

Email Security

Emails can contain malicious content and malware. To reduce harm, employees should employ the following strategies:

i. Do not open attachments or click any links where content is not well explained
ii. Check the email addresses and names of senders – validate that you know the sender and that it has the correct email address
iii. Search for inconsistencies/anomalies in both the email address and title
iv. Always block junk, spam, phishing, and scam emails – see O365 home screen ribbon
v. Avoid emails that contain common scam subject lines such as prizes, products, and money transfers

If an employee is not sure that an email, or any type of data is safe, the employee is required to open an IT Service Ticket via the Fresh Service Portal

Social Media

i. Personal use of social media is allowed and encouraged. However only authorized employees may speak out on behalf of the AAG on social media. All social media active employees should be aware that what they say on social media, if it pertains to the company, can have an impact on the company.
ii. Employees may not engage in social media regarding AAG business partners, products, employees, or any work-related matters, whether confidential or not, unless contained in a communication that has been authorized by a company spokesperson or the leadership team.
iii. In the employees' personal use of social media, they may not disclose or use their affiliation with the AAG in a manner that may be construed as them having access to confidential or business-sensitive information regarding the AAG or as if they are speaking on behalf of the company.
iv. Employees are expected to protect the privacy of AAG, its employees and its business partners and are prohibited from disclosing any proprietary and/or other non-public information to which employees have access due to their employment with AAG. Such information includes, but is not limited to, customer or consumer information, trade secrets, financial information, and strategic business plans.
v. For the protection, and the protection of AAG, employees using social media are expected to do so without infringing on the intellectual property rights of others. Employees are prohibited from engaging in any activities via social media that could provoke claims of infringement against the company.
vi. Employees are responsible to ensure that their online activities do not interfere with their job responsibilities.
vii. Employees should have no expectation of privacy when participating in social media. Postings can be viewed by anyone, including the AAG. The AAG reserves the right to monitor comments or discussions about the company, its employees, business partners and the industry.

Public Third-Party Services

i. Use of unauthorized messenger tools such as Facebook messenger, Skype, WhatsApp, etc for communicating confidential or secret information.
ii. Transfer any business documents with non-company provided file sharing or file storage tools is prohibited (like WeTransfer, Dropbox, SlideShare, etc.) – business documents shall only be transferred using tools and methods provided by the company.

Email Usage

i. The corporate email system is not for personal use.
ii. Sending unsolicited email messages, including the sending of "junk email" or other advertising materials (unless otherwise authorized) to individuals who did not specifically request such materials (email spam).
iii. Unauthorized use or forgoing of email header information.
iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or collect replies.
v. Creating or forwarding "chain letters", "Ponzi" or other "Pyramid" schemes of any type.
vi. Use of unsolicited originating from within AAG's networks of other internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by AAG or connected via AAG's network.

Device Security and Using Personal Devices

Logging in to any work accounts for personal devices such as mobile phones, tablets, or laptops, can put AAG data at risk. AAG does not recommend accessing any AAG data from personal devices. However, if this cannot be avoided, employees are obligated to keep their devices in a safe place and not exposed to anyone else.

Employees are recommended to follow these best practice steps:

i. Keep all electronic devices' passwords secure and protected
ii. Logging into accounts should only be performed through safe networks (note - beware of free Wi-Fi access points in public places)
iii. Security updates and endpoint protection will be managed on the AAG device by the IT Service team.
iv. Never leave devices unprotected and/or exposed
v. Close computers when leaving the desk.

Transferring Data

Employees should follow these best practices when transferring data:

i. Adhere to the relevant personal information legislation (see AAG – Privacy Policy)
ii. Data should only be shared over authorized networks
iii. We use encryption technologies to protect data at rest and in motion.
iv. If applicable, destroy any sensitive data when it is no longer required

To transfer data safely please reach out to the IT team directly for specific instructions.

Physical Documents

Employees are required to ensure that:

i. Printed documents containing sensitive and confidential information should be immediately removed from the printer
ii. Any sensitive and confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of each workday
iii. File cabinets containing sensitive and confidential information must be kept closed and locked when not in use or when not attended
iv. Keys used for access to sensitive and confidential information must not be left at an unattended desk
v. Upon disposal of sensitive and confidential documents, documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins
vi. Whiteboards containing sensitive and confidential information should be erased after use.

Working Remotely

When working remotely it is important:

i. Use a virtual private network (VPN) when connecting to the Internet to ensure your communications and online activities are encrypted and secure.
ii. Avoid using public Wi-Fi networks whenever possible, as they are often unsecured and can be easily hacked. If you must use public Wi-Fi, connect only to networks that are password-protected and encrypted.
iii. Never leave your devices unattended in a public place, even for a short period of time. This includes laptops, tablets, smartphones, and other mobile devices.
iv. Always lock your screen when you step away from your device and use a strong password or passcode to protect your device from unauthorized access.
v. Avoid accessing sensitive or confidential information, such as financial or personal data, when in a public place. If you must access such information, use a secure connection, and take extra precautions to ensure that your screen is not visible to others.
vi. Be mindful of your surroundings when using your device in a public place. Avoid conversations or activities that could reveal sensitive information and be cautious of anyone who may be trying to eavesdrop on your activities.
vii. Keep your software and security systems up to date to ensure that your device is protected against the latest threats and vulnerabilities.

viii. Regularly back up your data to a secure location to prevent data loss in case of theft or other security incidents.
ix. Report any suspected security incidents, such as theft or hacking, to the appropriate authorities and your employer immediately.

Follow your employer's policies and procedures for working remotely or in public places and seek guidance from your supervisor or IT department if you have any questions or concerns about cyber security.

Acceptable Use

i. User accounts on work systems are only to be used for the business purposes of the AAG and not to be used for personal activities.
ii. Employees are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords.

Unacceptable Use

i. Employees are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the AAG.
ii. Employees must not purposely engage in any activity with the intent to: harass other users, degrade the performance of the network/systems, divert system resources to their own use, or gain access to AAG systems for which they do not have authorization.
iii. Installation of private or non-corporate software on a company owned computer (i.e., software that is not provided and licensed by AAG. All software applications must only be installed by IT.
iv. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources.
v. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
vi. Introduce programs into the network or server that may contain malicious viruses, worms, trojan horses, email-bombs etc.
vii. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being undertaken at home.
viii. Making fraudulent offers of products, items, or services originating from any AAG account.
ix. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

x. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to , network sniffing, pinging floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

xi. Port scanning or security scanning is expressly prohibited unless prior notification to the Group IT or Chief Transformation Officer at AAG is made.

Security Requirements

i. Non privileged users may not install unauthorized software.

ii. Employees must not use unauthorized devices on their workstations unless they have received specific authorization from the Chief Transformation Officer.

iii. Employees must not attempt to turn off or circumvent any security measures.

iv. Employees must report any security breaches, suspicious activities or issues that may cause a Cyber Security breach to aagITsecurity@activeapparel.com.au

Policy Enforcement

In the event the employee is found to have violated these Terms of Use or any related policy, procedure, manual or guideline, AAG reserves the right to take appropriate actions to rectify the situation in relation to the security and circumstances in question.
Repeated violations will substantiate an escalation to a higher remedial action. These actions could include removal of the AAG owned computer or mobile device or disciplinary sanctions in accordance with any existing workplace regulations and agreements and local labour laws.

If this policy is breached, one or more of the following disciplinary actions will take place:

i. Incidents will be assessed on a case-by-case basis

ii. In cases of breaches that are intentional or repeated or cases that cause direct harm to the AAG, employees may face serious disciplinary action

iii. Subject to the gravity of the breach, formal warnings may be issued to the offending employee.

Companion Policies

The following Policies work in tandem with the AAG Information Security Policy:

11.1 Privacy Policy

11.2 Guest & Third-Party Access Policy

11.3 Domain & Whitelisting Policy

Whistle Blower Policy

Version	Modification Date	Last Modified By	Document Changes
0.1	17/11/2022	Terence Wallis	Initial Draft of the Whistle Blower policy
1.0	20/01/2023	Terence Wallis	Sent for review & approval
2.0	2/03/2023	Terence Wallis	Updated and added additional information
3.0	20/03/2023	Terence Wallis	Updated Advisor to the Board contact

Introduction

At the Active Apparel Group (AAG), we are guided by our values which provides a compass on how we do business. AAG is committed to ensuring corporate compliance and promoting an ethical culture by observing the highest standards of fair dealing, honesty, and integrity in our business activities.
AAG encourages the reporting of any instances of suspected unethical, illegal, corrupt, fraudulent, or undesirable conduct involving the AAG business and provides protections and measures to individuals who make a disclosure in relation to such conduct without the fear or victimization or reprisal.
This policy will be made available on our website and in any other ways that will ensure that it is made available to persons to whom this policy applies.

Objective

The objective of this policy is to encourage reporting of wrongdoing that is of legitimate concern by providing a convenient and safe reporting mechanism, and protection for people who make serious wrongdoing disclosures.

Purpose

The purpose of the Whistle Blower policy is to:

i. Outline how and to whom employees should report their concerns, as well as the process that will be followed to investigate the allegations.

ii. Its goal is to encourage employees to come forward with concerns without fear of retaliation.

iii. It also ensures that if there are any consequences for reporting, they are evenly distributed throughout the company.

iv. Policies are usually enforced through an employee handbook or other company policies.

Scope

AAG wants to ensure that all employees have confidence and surety that if they report a concern that all allegations will be investigated thoroughly and without bias.

This policy applies to:

i. All employees of AAG
ii. Suppliers (including vendors, contractors, consultants, or service providers)
iii. A relative, dependent or spouse of any of the above.

If an individual qualifies as any of the above and:

i. Makes a disclosure of information relating to a 'disclosable matter' directly to any 'eligible recipient'.
ii. Has made a disclosure to a legal practitioner for the purposes of obtaining legal advice or legal representation about the operation of the whistle-blower provisions in the Corporations Act; or
iii. Has made an 'emergency disclosure' or 'public interest disclosure'.

They will qualify for protection as a whistle-blower under this policy and the Corporations Act.

To help enable this the following must be in place:

i. The Whistle Blower policy must be publicly accessible and prominently displayed throughout the workplace.
ii. It includes an assurance that all reports will be taken seriously and investigated thoroughly and promptly – regardless of their source.
iii. US employees can go through their employer's internal complaint process or file a claim with the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA).
iv. Australian employees can go through their employer's internal complaint process or file a claim with the Australian Securities & Investments Commission.

Reportable Conduct

You may make a report or disclosure under this Policy if you have reasonable grounds to believe that a company director, officer, employee, contractor, supplier, consultant, or other person who has business dealings with AAG has engaged in conduct (Reportable Conduct) which is:

i. Dishonest, fraudulent, or corrupt
ii. Illegal (such as theft, dealing in or use of illicit drugs, violence or threatened violence and criminal damage to property)
iii. Unethical

iv. Oppressive or grossly negligent
v. Potentially damaging to AAG, its employees or a third party
vi. Misconduct or an improper state of affairs
vii. A danger, or represents a danger to the public or financial system

For the avoidance of doubt, Reportable Conduct does not include personal work-related grievances.

A personal work-related grievance is a grievance about any matter in relation to an employee's current or former employment, having implications (or tending to have implications) for that person personally and that do not have broader implications for AAG.

Examples of personal work-related grievances are as follows:

i. An interpersonal conflict between the employee and another employee
ii. A decision relating to the engagement, transfer, or promotion of the employee
iii. A decision relating to the terms and conditions of engagement of the employee
iv. A decision to suspend or terminate the engagement of the employee, or otherwise to discipline the employee

Making a disclosure

AAG relies on its employees maintaining a culture of honest and ethical behaviour. Accordingly, if an eligible Whistle Blower becomes aware of any Reportable Conduct, it is expected that they will make a disclosure under this Policy.

There are several ways in which you may report or disclose any issue or behaviour which you consider to be Reportable Conduct.

Internal Reporting

You may disclose any Reportable Conduct to any of the Whistle Blower Protection Officers listed below:

- Special Advisor – Board of Directors

These Officers will safeguard your interests and will ensure the integrity of the reporting mechanism. If you are unable to use any of the above reporting channels, a disclosure can be made to one of the following within AAG.

- Board Members
- Officers
- Directors

Anonymity

When making a disclosure, you may do so anonymously.

It may be difficult for AAG to thoroughly investigate the matters disclosed if a report is submitted anonymously and therefore, we encourage you to share your identity when making a disclosure, however you are not required to do so.

Investigation

AAG will investigate all matters reported under this Policy as soon as practicable after the matter has been reported.

The Whistle Blower Protection Officer will investigate the matter and where necessary, appoint an internal or external investigator to assist in conducting the investigation.

All investigations will be conducted in a fair, independent, and timely manner and all reasonable efforts will be made to preserve confidentiality during the investigation.

If the report is not anonymous, the Whistle Blower Protection Officer or investigator will contact you to discuss the investigation process and any other matters that are relevant to the investigation.

Where you have chosen to remain anonymous, your identity will not be disclosed to the investigator or to any other person and AAG will conduct the investigation based on the information provided to it.

Where possible, the Whistle Blower Protection Officer will provide you with feedback on the progress and expected timeframes of the investigation. The person(s) against whom any allegations have been made will also be informed of the concerns and will be provided with an opportunity to respond (unless there are any restrictions or other reasonable bases for not doing so).

To the extent permitted by law, the Whistle Blower Protection Officer may inform you and/or a person against whom allegations have been made of the findings.

Any report will remain the property of AAG and will not be shared with you or any person(s) against whom the allegations have been made.

Protection of Whistle Blowers

AAG is committed to ensuring that any person who makes a disclosure is treated fairly, does not suffer detriment, and that confidentiality is preserved in respect of all matters raised under this Policy.

Protection against Legal Action

You will not be subject to any civil, criminal, or administrative legal action (including disciplinary action) for making a disclosure under this Policy or participating in any investigation.

Any information you provide will not be admissible in any criminal or civil proceedings other than for proceedings in respect of the falsity of the information.

Protection against detrimental conduct

AAG (or any person engaged by AAG) will not engage in 'Detrimental Conduct' against you if you have made a disclosure under this Policy.
Detrimental Conduct includes actual or threatened conduct such as the following (without limitation):

i. Termination of employment
ii. Injury to employment including demotion, disciplinary action
iii. Alternation of position or duties
iv. Discrimination
v. Harassment, bullying or intimidation
vi. Victimisation
vii. Harm or injury including psychological harm
viii. Damage to person's property
ix. Damage to a person's reputation
x. Damage to a person's business or financial position
xi. Any other damage to a person

AAG will take all reasonable steps to protect you from Detrimental Conduct and will take necessary action where such conduct is identified.

AAG also strictly prohibits all forms of Detrimental Conduct against any person who is involved in an investigation of a matter disclosed under the Policy in response to their involvement in that investigation.

If you are subjected to Detrimental Conduct as a result of making a disclosure under this Policy or participating in an investigation, you should inform a Whistle

Blower Protection Officer or eligible recipient in accordance with the reporting guidelines outlined above.

You may also seek remedies including compensation, civil penalties, or reinstatement where you have been subject to any Detrimental Conduct.

Protection of Confidentiality

All information received from you will be treated confidentially and sensitively.

If you make a disclosure under this Policy, your identity (or any information which would likely to identify you) will only be shared if:

- You give your consent to share that information
- The disclosure is allowed or required by law (for example where the concern is raised with a lawyer for the purposes of obtaining legal advice)

Where it is necessary to disclose information for the effective investigation of the matter, and this is likely to lead to your identification, all reasonable steps will be taken to reduce the risk that you will be identified.

False or Misleading Reporting

Where the information received is found to be:

- Trivial or vexatious in nature with no substance
- Unsubstantiated, and found to be made maliciously
- Made knowingly to be false

This will be treated in the same manner as a false report and may itself constitute wrongdoing.

These actions will be taken seriously and may result in disciplinary action, up to and including termination of employment.

Breach of Policy

This Policy and its application are at AAG's discretion (subject to AAG complying with statutory obligations) and may be varied, withdrawn, or replaced from time to time.

This Policy is not intended to constitute a contractual term or a contractual promise.

How to make Whistle Blower Disclosure

You are able to make a report (disclosure) by submitting your details by any of the WPO's or Eligible Recipients.

Please ensure you include clear details of the breach; what happened, where and when.

Please provide supporting evidence of your disclosure and the names of any other persons involved.

A disclosure can also be made anonymously; however, this can make the disclosure more difficult to investigate and AAG will not be able to respond to you personally.

Reports can be made by post marked **Confidential** :

Attention: Advisor to the Board
Active Apparel Group
Level 2, 365 Macarthur Avenue
Hamilton. QLD 4007
Australia

Attention: Advisor to the Board
Active Apparel Group
Suite 100
6059 Bristol Parkway
Culver City. CA 90230
United States of America

Reports can also be made via email: advisortotheboard@activeapparel.com.au

Notification of Changes

The Company reserves the right to amend AAG Code of Ethics from time to time and for any reason, at our sole discretion, by updating this handbook. If the Company decides to change this policy, Workers will be made aware.