DATA BREACH & INCIDENT RESPONSE POLICY

Document Owner: All About Ads® (A Cube Group Company)
Approved By: Managing Director / Authorized Signatory
Version: 1.0
Effective Date: 01-04-2026
Review Frequency: Annually or following a significant security or privacy incident.

---

1. Purpose

The purpose of this Policy is to establish a structured process for identifying, reporting, assessing, managing, and responding to actual or suspected information security incidents and personal data breaches involving All About Ads® ("the Company").

The Company is committed to minimizing the impact of security incidents, protecting stakeholder interests, maintaining client trust, and fulfilling applicable legal and contractual obligations.

---

2. Scope

This Policy applies to:

- All employees, consultants, freelancers, interns, and temporary employees;
- Personal Data processed by or on behalf of the Company;
- Company-owned devices and systems;
- Cloud-based collaboration platforms and business applications used for service delivery;
- Third parties engaged in support of contracted services.

---

3. Definitions

Information Security Incident

Any event that compromises or has the potential to compromise the confidentiality, integrity, or availability of Company or client information.

Examples include:

- Unauthorized access to systems or files;
- Lost or stolen devices containing business information;
- Malware or ransomware infections;
- Accidental disclosure of confidential information;
- Phishing attacks;
- Unauthorized use of credentials.

Personal Data Breach

Any incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

---

4. Reporting Responsibilities

All employees must immediately report any actual or suspected information security incident to their reporting manager or designated management representative.

Incidents should be reported as soon as reasonably practicable and should include:

- Description of the incident;
- Date and time identified;
- Type of information involved;
- Individuals or systems potentially affected;
- Immediate actions taken.

Failure to report known incidents may result in disciplinary action.

---

5. Incident Response Process

Step 1 – Identification

The incident shall be identified and documented by the individual discovering the event.

Step 2 – Escalation

The matter shall be promptly escalated to management for review and coordination.

Step 3 – Assessment

Management shall assess:

- Nature and severity of the incident;
- Type of information involved;
- Whether Personal Data is affected;
- Number of individuals potentially impacted;
- Potential operational, legal, contractual, or reputational consequences.

Step 4 – Containment

Reasonable steps shall be taken to contain the incident and prevent further unauthorized access or disclosure.

Examples include:

- Revoking system access;

- Recovering misplaced records;
- Isolating affected devices;
- Changing compromised credentials.

Step 5 – Investigation

An investigation shall be undertaken to determine:

- Root cause;
- Extent of impact;
- Corrective actions required.

Step 6 – Notification

Where required by applicable law, contractual obligations, or client requirements, relevant stakeholders may be notified, including:

- Clients or agencies;
- Service providers;
- Legal advisors;
- Regulatory authorities.

Notifications shall be coordinated through management.

Step 7 – Remediation

Appropriate corrective actions shall be implemented to reduce the likelihood of recurrence.

---

6. Third-Party Incidents

Where a third party engaged by the Company experiences an incident affecting Company or client information, the incident shall be escalated to management immediately upon becoming aware of the event.

The Company shall coordinate with the relevant client or agency, where appropriate.

---

7. Documentation

The Company shall maintain an Incident Register containing:

- Date of incident;
- Nature of incident;
- Impact assessment;
- Actions taken;
- Notification decisions;

- Corrective measures implemented;
- Closure date.

---

8. Training and Awareness

Employees shall be encouraged to promptly report suspected incidents without fear of retaliation.

Management shall periodically reinforce awareness regarding the importance of incident reporting and information security responsibilities.

---

9. Policy Review

This Policy shall be reviewed annually or following any material security incident, changes in business operations, or changes in applicable legal or contractual requirements.

Approved By: _____

Name: _____

Designation: _____

Date: _____

DATA RETENTION & DISPOSAL POLICY

Document Owner: All About Ads® (A Cube Group Company)
Approved By: Managing Director / Authorized Signatory
Version: 1.0
Effective Date: 01-04-2026

Review Frequency: Annually or upon significant changes in legal, contractual, or operational requirements.

---

1. Purpose

The purpose of this Policy is to establish principles for the retention, review, disposal, and deletion of information and Personal Data processed by All About Ads® ("the Company").

The Company is committed to retaining information only for as long as necessary to fulfil legitimate business purposes, contractual obligations, and applicable legal requirements.

---

2. Scope

This Policy applies to:

- Employees, consultants, interns, freelancers, and temporary employees;
- Personal Data processed by the Company;
- Client information and project-related records;
- Electronic and physical records maintained by the Company.

---

3. Retention Principles

The Company shall:

- Retain information only for legitimate business, contractual, legal, or operational purposes;
- Limit retention to the minimum period reasonably necessary;
- Periodically review retained information;
- Securely dispose of information that is no longer required.

---

4. Retention Categories

4.1 Client Project Information

Project records, reports, presentations, photographs, videos, and operational documentation may be retained for business continuity, reference, audit support, contractual obligations, and portfolio purposes.

Retention Period:
As required by contractual obligations or business necessity.

4.2 Event Registration and Activation Data

Personal Data collected during events, activations, and campaigns shall be retained only for the duration necessary to fulfil the agreed purpose, complete reporting obligations, and provide deliverables to the relevant client or agency.

Retention Period:
Deleted or securely disposed of once no longer required for the relevant engagement, unless otherwise instructed by the client or required by law.

4.3 Financial and Commercial Records

Invoices, contracts, purchase orders, tax records, and related commercial documentation shall be retained in accordance with applicable statutory requirements.

Retention Period:
As required under applicable laws and regulations.

4.4 Human Resources Records

Employees records shall be retained in accordance with applicable employment laws and legitimate business requirements.

Retention Period:
As required under applicable laws and regulations.

---

5. Disposal of Information

Where information is no longer required, reasonable steps shall be taken to ensure secure disposal.

Disposal methods may include:

- Permanent deletion from electronic systems;
- Removal from cloud-based storage platforms;
- Secure disposal of physical records;
- Destruction of redundant copies where appropriate.

---

6. Personal Data Deletion Requests

Where applicable, requests relating to the deletion of Personal Data shall be reviewed in accordance with:

- Applicable laws;
- Contractual obligations;
- Client instructions;
- The Company's role as a Data Controller or Data Processor.

Where Personal Data is processed on behalf of a client, deletion requests may be referred to the relevant client or agency.

---

7. Responsibilities

Employees are responsible for:

- Maintaining records appropriately;
- Avoiding unnecessary duplication of information;
- Complying with approved retention and disposal practices.

Management shall oversee the implementation and periodic review of this Policy.

---

8. Exceptions

Information subject to:

- Ongoing legal proceedings;
- Regulatory investigations;
- Audit requirements;
- Client preservation instructions;

shall not be disposed of until the relevant matter has been resolved.

---

9. Policy Review

This Policy shall be reviewed annually or whenever significant changes occur in legal requirements, business operations, or contractual obligations.

Approved By: _____

Name: _____

Designation: _____

Date: _____

INFORMATION SECURITY POLICY

1. Purpose

The purpose of this Information Security Policy is to establish a framework for protecting the confidentiality, integrity, and availability of information assets managed by All About Ads® ("the Company"). This policy outlines the principles and responsibilities for safeguarding company, client, supplier, and project-related information against unauthorized access, disclosure, alteration, loss, or misuse.

2. Scope

This policy applies to:

- All employees, directors, consultants, interns, freelancers, and temporary staff of the Company.
- All information assets owned, processed, or managed by the Company.
- All devices, systems, applications, cloud platforms, and communication channels used for business purposes.

3. Information Security Principles

The Company is committed to:

- Protecting information against unauthorized access.
- Ensuring information accuracy and integrity.
- Maintaining the availability of critical business information.
- Complying with applicable legal, contractual, and regulatory obligations.
- Promoting security awareness among employees.

4. Access Control

- Access to information shall be granted on a need-to-know basis and aligned with job responsibilities.
- Individual user accounts shall be used wherever practicable.
- Password-protected access shall be required for business systems and devices.
- User access rights shall be reviewed periodically and modified or revoked when roles or responsibilities change.

5. Acceptable Use

Employees shall:

- Use company systems and information solely for legitimate business purposes.
- Exercise due care when handling client and confidential information.
- Refrain from sharing passwords or unauthorized access credentials.
- Avoid installing unauthorized software or applications on company devices.

6. Information Classification and Handling

Information shall be handled according to its sensitivity and business value. Confidential information, including client data and commercial information, shall only be shared with authorized individuals involved in the relevant engagement.

7. Third-Party Access

Third parties granted access to company or client information shall receive only the minimum access necessary to perform their duties. Confidentiality obligations shall be established where appropriate.

8. Incident Reporting

All employees are required to promptly report any suspected information security incidents, unauthorized access, loss of devices, or accidental disclosure of information to management for assessment and appropriate action.

9. Security Measures

The Company shall implement security measures appropriate to the nature and scale of its operations, including:

- Password-protected systems and devices.
- Use of secure business collaboration platforms.
- Controlled access to project information.
- Periodic review of user access rights.
- Security awareness and management oversight.

10. Compliance

Failure to comply with this policy may result in disciplinary action and other measures deemed appropriate by the Company.

11. Policy Review

This policy shall be reviewed annually or whenever significant changes occur in business operations, technology environments, or applicable legal and contractual requirements.

Approved By: _____

Name: _____

Designation: _____

Date: _____

PRIVACY POLICY

Document Owner: All About Ads® (A Cube Group Company)
Approved By: Managing Director / Authorized Signatory
Version: 1.0
Effective Date: 01-04-2026
Review Frequency: Annually or upon significant changes in applicable legal, regulatory, or contractual requirements.

---

1. Purpose

The purpose of this Privacy Policy is to establish principles and responsibilities for the collection, processing, use, disclosure, retention, and protection of Personal Data handled by All About Ads® ("the Company") in connection with its business activities.

The Company is committed to respecting the privacy rights of individuals and processing Personal Data in a lawful, fair, transparent, and secure manner.

---

2. Scope

This Policy applies to:

- Directors, employees, consultants, temporary staff, and contractors of the Company;
- Personal Data processed in connection with the Company's services, operations, and business relationships;
- Personal Data processed on behalf of clients and agencies.

---

3. Types of Personal Data Processed

The Company may process limited categories of Personal Data, including:

- Full Name;
- Business Email Address;
- Personal Email Address (where voluntarily provided);
- Telephone Number;
- Age (where relevant to campaign requirements);
- Photographs and video recordings captured during events and activations;
- Event registration information;
- Other information necessary for the delivery of contracted services.

The Company does not intentionally collect or process sensitive personal data unless specifically required for a legitimate business purpose and authorized by the relevant client.

---

4. Purpose of Processing

Personal Data may be processed for purposes including:

- Event registration and attendance management;
- Brand activations and experiential programs;
- Campaign execution and reporting;
- Lead collection activities authorized by clients;
- Communication relating to events and campaigns;
- Compliance with contractual obligations;
- Business administration and operational management.

---

5. Lawful Basis

Where applicable, Personal Data shall be processed based on one or more of the following:

- Performance of contractual obligations;
- Legitimate business interests;
- Compliance with legal obligations;
- Instructions received from clients or agencies acting as Data Controllers;
- Consent, where required by applicable law.

---

6. Data Sharing

The Company may share Personal Data with:

- Clients and agencies engaging the Company;
- Service providers supporting the delivery of contracted services;
- Regulatory authorities where required by law.

Personal Data shall only be shared to the extent necessary for legitimate business purposes.

---

7. Data Retention

Personal Data shall be retained only for as long as necessary to fulfil the purpose for which it was collected, comply with contractual obligations, satisfy legal requirements, or address legitimate business needs.

When Personal Data is no longer required, reasonable steps shall be taken to securely delete or dispose of such information.

---

8. Information Security

The Company implements reasonable administrative and operational safeguards appropriate to the nature and scale of its operations to protect Personal Data against unauthorized access, disclosure, alteration, or loss.

Access to Personal Data shall be restricted to authorized employees on a need-to-know basis.

---

9. Data Subject Requests

Where applicable, requests relating to access, correction, deletion, or other privacy rights shall be reviewed in accordance with applicable laws, contractual obligations, and the Company's role as a Data Processor or Data Controller.

Where the Company processes Personal Data on behalf of a client, such requests may be referred to the relevant client or agency.

---

10. Data Breaches

Any suspected Personal Data breach shall be promptly escalated to management for assessment, containment, and appropriate action, including notification to relevant stakeholders where required.

---

11. Children's Data

The Company does not intentionally collect or process children's Personal Data as part of its standard service offerings.

Where children form part of an audience during events or campaigns, appropriate care shall be exercised to avoid the unnecessary collection of Personal Data relating to children.

---

12. Responsibilities

All employees are responsible for:

- Protecting Personal Data entrusted to the Company;
- Following applicable policies and procedures;
- Reporting suspected privacy incidents without delay.

Management shall oversee the implementation and periodic review of this Policy.

---

13. Policy Review

This Policy shall be reviewed annually or whenever material changes occur in the Company's operations, legal obligations, or contractual requirements.

Approved By: _____

Name: _____

Designation: _____

Date: _____

RESPONSIBLE ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY

Document Owner: All About Ads® (A Cube Group Company)
Approved By: Managing Director / Authorized Signatory
Version: 1.0
Effective Date: 01-04-2026

Review Frequency: Annually or upon significant changes in technology, legal requirements, client expectations, or business operations.

---

1. Purpose

The purpose of this Policy is to establish principles governing the responsible use of Artificial Intelligence ("AI") technologies within All About Ads® ("the Company").

The Company recognizes the potential of AI to enhance creativity, efficiency, and innovation while also acknowledging the importance of maintaining human oversight, protecting confidentiality, respecting intellectual property rights, and complying with applicable legal and contractual obligations.

This Policy seeks to ensure that AI technologies are used ethically, responsibly, and in a manner consistent with the Company's values and professional standards.

---

2. Scope

This Policy applies to:

- Directors, employees, consultants, freelancers, interns, and temporary employees engaged by the Company;
- All AI-enabled tools, platforms, and applications used in connection with Company business activities;
- AI-generated outputs intended for internal use or external delivery to clients.

---

3. Approved Uses of Artificial Intelligence

The Company may utilize AI technologies to support business activities including, but not limited to:

- Creative ideation and brainstorming;
- Campaign concept development;
- Content drafting and refinement;
- Presentation development and design support;
- Creative visualization and mood board creation;
- Image generation for conceptual purposes;
- Research support and information summarization;

- Internal productivity and efficiency enhancement.

AI shall be used as an assistive tool and not as a substitute for professional judgment.

---

4. Human Oversight and Accountability

All AI-generated outputs intended for client delivery, publication, presentation, or business decision-making shall be reviewed by an appropriately authorized employee before use.

Employees remain responsible for:

- Accuracy of final outputs;
- Suitability for the intended purpose;
- Compliance with applicable laws and regulations;
- Compliance with client requirements;
- Protection of confidential information.

The use of AI does not transfer accountability from individuals to technology providers.

---

5. Protection of Confidential and Personal Information

Employees shall not intentionally input the following into publicly accessible AI systems without appropriate authorization and safeguards:

- Client confidential information;
- Personal Data collected during campaigns or activations;
- Proprietary business information;
- Financial information;
- Commercially sensitive information;
- Information subject to confidentiality obligations.

Where AI tools are used, users shall exercise reasonable care to minimize privacy and confidentiality risks.

---

6. Prohibited Uses

The Company prohibits the use of AI technologies for:

- Processing Personal Data for model training purposes;
- Automated decision-making affecting individuals without appropriate review;
- Creation of deceptive, fraudulent, discriminatory, or unlawful content;
- Circumvention of legal, regulatory, or contractual obligations;

- Activities that may harm the reputation of the Company or its clients.

---

7. Intellectual Property Considerations

Employees using AI-generated content shall exercise reasonable care to ensure that outputs do not knowingly infringe third-party intellectual property rights.

Where AI-generated materials are used externally, employees should assess whether additional verification, attribution, licensing review, or modification is appropriate.

---

8. Transparency and Client Requirements

Where required by:

- Applicable law;
- Contractual obligations;
- Client instructions;

the Company shall provide appropriate transparency regarding the use of AI technologies in connection with service delivery.

The Company acknowledges that certain clients may establish specific restrictions or approval requirements relating to the use of AI tools.

---

9. Approved AI Platforms

The Company may authorize the use of AI platforms that support legitimate business purposes.

Examples may include:

- OpenAI ChatGPT;
- Google Gemini;
- AI-enabled presentation tools;
- AI-assisted creative and image generation platforms;
- Other platforms approved by management.

Employees shall avoid using unapproved AI tools for business purposes where they present material privacy, confidentiality, or security concerns.

---

10. Training and Awareness

Employees shall be encouraged to:

- Understand the strengths and limitations of AI technologies;
- Apply critical thinking when reviewing AI-generated outputs;

- Escalate concerns relating to inappropriate or potentially harmful AI usage.

Management shall periodically review emerging risks and opportunities associated with AI adoption.

---

11. Compliance

Failure to comply with this Policy may result in disciplinary action and other measures deemed appropriate by the Company.

---

12. Policy Review

This Policy shall be reviewed annually or earlier where:

- Significant changes occur in the Company's use of AI;
- Material legal or regulatory developments arise;
- Client requirements necessitate policy updates.

Approved By: _____

Name: _____

Designation: _____

Date: _____