INNERMEDIA

25

YEARS · 2001–2026

INFORMATION SECURITY POLICY

TERMS, CONDITIONS & POLICIES

VERSION 4.0 · MAY 2026

INNER MEDIA LIMITED · COMPANY NO. 04818830
SOPERS HOUSE, SOPERS RD, CUFFLEY, POTTERS BAR EN6 4RY
01707 875 721 · INNERMEDIA.CO.UK

POLICY DETAIL	INFORMATION
Policy Owner	Board of Directors
Approved By	Board of Directors
Review Cycle	Annual (or following a significant security incident)
Applies To	All InnerMedia staff, contractors and any third party with access to InnerMedia systems
Associated Documents	Data Protection Policy | Privacy Policy | AI & Data Transparency Statement | DPA
Regulatory Framework	UK GDPR | Data Protection Act 2018 | Computer Misuse Act 1990 | Network and Information Systems (NIS) Regulations 2018

1. INTRODUCTION

1.1 Information security is fundamental to InnerMedia's ability to deliver trusted services to our clients. We hold sensitive data on behalf of schools, businesses and their communities. Protecting that data is a legal obligation and a commercial and ethical responsibility.

1.2 This policy establishes InnerMedia's information security framework, based on the CIA triad:

- Confidentiality — data is accessible only to those with authorised need;
- Integrity — data is accurate, complete and protected from unauthorised alteration;
- Availability — data and systems are available to authorised users when needed.

1.3 Compliance with this policy is mandatory for all staff. Contractors and sub-processors must comply with equivalent standards as a condition of their engagement.

2. SCOPE

This policy applies to all information assets owned, managed or processed by InnerMedia, including:

- Client data and Personal Data;
- AI product infrastructure and configurations;
- InnerMedia's internal systems, networks and devices;

- Third-party systems accessed in connection with InnerMedia services (AWS, WordPress, SendGrid, etc.);
- Physical documents containing sensitive information.

3. RESPONSIBILITIES

3.1 Board of Directors

The Board holds ultimate accountability for information security. The Board shall ensure that appropriate resources are allocated, that this policy is reviewed annually, and that significant incidents are escalated appropriately.

3.2 Information Security Lead

The Information Security Lead (currently the Managing Director) is responsible for:

- Day-to-day oversight of security controls and compliance;
- Maintaining the risk register and reviewing it quarterly;
- Approving new information systems before deployment;
- Managing security incidents and coordinating response;
- Overseeing staff security training.

3.3 All Staff

- Follow all security controls and procedures in this policy;
- Report suspected security incidents or breaches immediately to the Information Security Lead;
- Complete security training at induction and annually;
- Not share passwords, access credentials or security tokens;
- Lock screens when away from their workstation;
- Not install unapproved software on company or client systems.

4. ACCESS CONTROLS

4.1 Principles

Access to InnerMedia systems and client data shall be granted on the principle of least privilege — each user shall have access only to the information and systems necessary for their role, and no more.

4.2 User Access Management

- All user accounts must be individually assigned — shared accounts are prohibited;
- Access rights must be reviewed quarterly and when roles change;
- Access must be revoked within 24 hours of a staff member leaving or changing role;
- Privileged access (admin rights, database access, AI configuration access) requires explicit approval from the Information Security Lead and must be logged.

4.3 Passwords

- All passwords must be a minimum of 12 characters, combining upper and lower case letters, numbers and symbols;
- Passwords must not be reused across systems;
- Staff are required to use Last Pass a company-approved password manager;
- Passwords must be changed immediately if compromise is suspected.

4.4 Multi-Factor Authentication (MFA)

MFA is mandatory for all InnerMedia systems and all systems where
client data is accessible. There are no exceptions. If a system does
not support MFA, it must not be used to access or store personal data
without explicit Board approval.

- MFA must be enabled on: all cloud systems (AWS, Microsoft 365, Google Workspace); CMS and hosting management portals; email accounts; AI configuration platforms; any system containing client or personal data.

5. DEVICE AND EQUIPMENT SECURITY

5.1 Company and Personal Devices

- All company-issued devices must have full-disk encryption enabled;
- Personal devices (BYOD) used for work must have screen lock, encryption, and remote wipe capability enabled;
- Screens must be locked when unattended (maximum idle lock: 5 minutes);
- Devices must not be left unattended in public places without being locked or stored securely.

5.2 Remote Working

- Public Wi-Fi networks must not be used to access client data or InnerMedia systems without VPN;
- Staff must ensure their home networks are secured with WPA2 or WPA3 encryption;
- Video calls involving client data must not be conducted in public spaces.

5.3 Device Disposal

All storage media (hard drives, USB drives, mobile devices) must be securely wiped or physically destroyed before disposal. The Information Security Lead must confirm disposal and maintain a record.

6. NETWORK AND CLOUD SECURITY

6.1 AWS Infrastructure

- All InnerMedia production systems run on Amazon Web Services (AWS) UK or EU regions;
- Data at rest is encrypted using AES-256;
- Data in transit is encrypted using TLS 1.2 or higher;
- AWS security groups and IAM policies restrict access to authorised services and users only;
- AWS CloudTrail and logging are enabled to record all API activity;
- Regular review of AWS IAM permissions to remove stale or overprivileged roles.

6.2 AI Infrastructure Security

- Anthropic Claude is accessed exclusively via our company account, not personal accounts
- Each client's AI configuration is logically isolated and not accessible to other clients;
- Prompt injection attack mitigation is implemented in all AI product configurations;
- AI conversation logs are stored in encrypted form and automatically deleted after360 days.

6.3 Third-Party Systems

SYSTEM	SECURITY CONTROLS
AWS (UK/EU)	AES-256 at rest, TLS 1.2+ in transit, MFA, IAM, CloudTrail logging
Microsoft 365 / OneDrive	MFA required, UK/EU data residency, conditional access policies
WordPress	Plugin updates maintained, admin access restricted to named users, MFA enabled

SYSTEM	SECURITY CONTROLS
SendGrid	API key rotation every 90 days, restricted sending permissions
Google Workspace	MFA required, EU data processing terms
Xero / Access Paysuite	MFA required, access limited to finance staff only

7. SOFTWARE AND PATCH MANAGEMENT

- All software must be kept up to date with security patches applied within 14 days of release for critical patches and 30 days for standard patches;
- Software must be sourced from official, verified sources only;
- No software may be installed on company devices or InnerMedia systems without approval from the Information Security Lead;
- WordPress plugins and themes must be reviewed and updated monthly; unused plugins must be deactivated and removed;
- End-of-life software must be replaced before vendor security support ends.

8. MALWARE AND THREAT PROTECTION

- Anti-malware software must be installed and kept up to date on all company devices;
- Email filtering and anti-phishing controls must be active on all email accounts;
- Staff must not click links or open attachments from unknown or suspicious sources;
- Removable media (USB drives) from external sources must not be used on InnerMedia systems without explicit approval and virus scanning;
- Staff must report phishing attempts to the Information Security Lead immediately.

9. PHYSICAL SECURITY

- Physical access to any workspace containing sensitive data must be controlled;
- Sensitive documents must not be left unattended;
- Printed documents containing personal data must be shredded (cross-cut) before disposal;

- Clean desk policy applies — sensitive information must be secured at end of working day.

10. SECURITY INCIDENT MANAGEMENT

ANY suspected security incident — however minor — must be reported to the Information Security Lead immediately. Do not investigate or attempt to resolve an incident independently.

10.1 What to Report

- Suspected or confirmed unauthorised access to any system or account;
- Loss or theft of any device containing business data;
- Receipt of suspicious emails (phishing, malware);
- Unexpected system behaviour that may indicate a breach;
- Accidental disclosure of personal data;
- AI product anomalies (unexpected outputs, data exposure).

10.2 Incident Response Process

- Contain: Immediately isolate affected systems or accounts to prevent further harm;
- Report: Notify the Information Security Lead within 1 hour;
- Assess: Information Security Lead assesses scope, severity and whether personal data is affected;
- Escalate: If personal data is affected, activate the Data Breach Response in the Data Protection Policy;
- Recover: Restore systems from clean backups where necessary;
- Review: Conduct a post-incident review within 5 Business Days and update controls as required;
- Document: Record all incidents in the Security Incident Register.

11. BUSINESS CONTINUITY AND DISASTER RECOVERY

11.1 InnerMedia's primary infrastructure is hosted on AWS, which provides built-in redundancy, automated backups and geographic resilience within UK/EU regions.

11.2 The following recovery objectives apply:

SYSTEM	RECOVERY POINT OBJECTIVE (RPO)
Client website hosting	24 hours
AI product infrastructure	1 hour
Internal systems (email, documents)	24 hours

11.3 Business continuity plans shall be tested at least annually by the Information Security Lead and reviewed following any significant incident.

12. RISK MANAGEMENT

12.1 The Information Security Lead maintains a Security Risk Register, reviewed quarterly. Risks are assessed by likelihood and impact and assigned to an owner for remediation.

12.2 Any new information system, AI feature or sub-processor must undergo a security risk assessment before deployment, including a Data Protection Impact Assessment (DPIA) where required under UK GDPR.

13. SUPPLIER AND SUB-PROCESSOR SECURITY

13.1 All suppliers and sub-processors with access to InnerMedia systems or client data must:

- Sign a Data Processing Agreement (DPA) or equivalent sub-processor agreement;
- Demonstrate compliance with appropriate security standards (ISO 27001, SOC 2, or equivalent);
- Report any security incident affecting InnerMedia data within 24 hours;
- Allow InnerMedia to audit their security controls on reasonable notice.

13.2 Supplier security shall be reviewed annually. Suppliers who cannot demonstrate adequate security shall be replaced.

14. STAFF TRAINING AND AWARENESS

- Security awareness training is mandatory at induction and annually;
- Staff working with AI products or client data must complete additional training;

- Phishing simulation exercises shall be conducted at least twice per year;
- Training completion records are maintained by the Information Security Lead.

15. POLICY REVIEW

This policy shall be reviewed annually by the Information Security Lead and approved by the Board. It shall also be reviewed following any significant security incident or material change to InnerMedia's systems or services.