Cobras AP

INFORMATION SECURITY POLICY

---

1. Statement of Policy

Cobras AP is committed to the highest standards of information security and treats data security and confidentiality extremely seriously.

This policy applies to all staff, including employees, directors, consultants, contractors, temporary and agency workers, trainees, casual and fixed-term staff, apprentices, interns, and volunteers.

All staff must familiarise themselves with and comply with this policy.

---

2. Purpose of Policy

Under the UK GDPR, Cobras AP must:

- Ensure the security of personal data against unlawful or unauthorised processing and accidental loss or destruction
- Demonstrate compliance through appropriate technical and organisational measures
- Protect against breaches of confidentiality, loss or misuse of assets and IT systems

This policy aims to:

- Protect confidential and business information
- Supplement the Data Protection and Security Policy
- Raise staff awareness of data security responsibilities

---

3. Definitions

- **Business Information**: Any Cobras AP business-related information not classed as personal data
- **Confidential Information**: Trade secrets or confidential data belonging to Cobras AP or third parties
- **Personal Data**: Information identifying an individual directly or indirectly
- **Sensitive Personal Data**: Data concerning health, racial/ethnic origin, politics, religion, sexual orientation, biometrics, etc.

4. Roles and Responsibilities

The Director has overall responsibility for implementing this policy, monitoring breaches, training staff, and ensuring UK GDPR compliance.

5. Scope

This policy applies to all written, verbal, and digital information processed by or on behalf of Cobras AP, including:

- Paper records
- Hand-held devices
- Telephones
- Computer systems
- Verbal communications

It also supplements key Cobras AP policies including:

- Employee & Consultant Privacy Notices
- Safeguarding
- Complaints
- HR
- Health and Safety
- Lone Working
- Diversity, Equity & Inclusion

6. General Principles

- Information is commercially valuable and must be protected
- Personal Data must be secured against unauthorised processing or accidental loss
- Only use data for specified, explicit and legitimate purposes
- Information is owned by Cobras AP and not for personal use

7. Information Management

- Personal Data must be accurate, relevant, and not retained longer than necessary
- Secure measures include:
    - Encryption
    - Strong passwords

    - Access controls

- Follow data retention and destruction policies

---

8. HR Information

- Personnel files are accessible only by HR unless role-specific access is granted
- Information must be kept confidential during recruitment, management, or supervision
- Staff may request access to their personnel files under the UK GDPR

---

9. Office Access & Information Handling

- Office keys and access codes must be secured
- Confidential materials must not be visible or accessible to unauthorised persons
- Visitors must:
    - Sign in
    - Be supervised at all times
    - Avoid access to sensitive data

---

10. Computers & IT

- Use encryption and password protection
- Lock devices when not in use
- Regularly back up data
- Do not copy Confidential Data to removable media without Director approval
- Avoid introducing malware; seek approval before installing software

---

11. Communications & Data Transfer

- Avoid speaking about confidential matters in public
- Mark sensitive materials as *"Strictly Private and Confidential"*
- Verify recipient details before sending information
- Encrypt sensitive data before email/postal transmission

---

12. Personal Email and Cloud Storage

- Do **not** use personal email or cloud storage (e.g., Gmail, iCloud) for work purposes
- Consult the Director if large-scale data transfer is required

13. Working from Home

- Only take information home when authorised
- Confidential data at home must be:
    - Locked away securely
    - Kept off personal devices
    - Disposed of securely

---

14. Transfers to Third Parties

- Only engage third parties with appropriate data security agreements
- Assess if they act as data processors under the UK GDPR
- Consult the Director when setting up or modifying such arrangements

---

15. International Data Transfers

- Personal Data must not be transferred outside the UK
- Refer to Cobras AP's Data Protection and Security Policy for details

---

16. Training

- Training is provided at induction and periodically thereafter
- Completion is mandatory
- Staff may request additional training from the Director

---

17. Reporting Data Breaches

All staff must report actual or potential data breaches to:

- Enable investigation and remediation
- Log incidents
- Notify regulatory authorities (e.g., ICO) if necessary

18. Non-Compliance

Cobras AP takes non-compliance seriously. Failure to follow this policy may result in disciplinary action, including dismissal.

For queries, contact the Director at info@cobrasap.co.uk

Last reviewed: June 2025