Data Protection Policies & Procedures

Policy Statement

The ExcluSec Group Ltd is committed to protecting the privacy, confidentiality and security of personal information. We recognise the importance of safeguarding personal data and ensuring that all processing activities are carried out lawfully, fairly and transparently.

The company processes personal information relating to employees, workers, applicants, clients, customers, suppliers, contractors, visitors, learners and members of the public as part of its normal business activities. This includes information collected through recruitment, employment, service delivery, training, CCTV systems, client contracts, compliance requirements and regulatory obligations.

All personal data will be handled in accordance with UK GDPR, the Data Protection Act 2018 and any other applicable legislation, guidance or regulatory requirements.

Purpose

The purpose of this policy is to establish the principles and standards that apply to the collection, use, storage, sharing, retention and disposal of personal data across the organisation.
This policy aims to:

- Protect the rights and freedoms of individuals whose personal data is processed by the company.
- Ensure compliance with UK data protection legislation.
- Promote accountability and transparency.
- Reduce the risk of data breaches and information security incidents.
- Provide guidance to employees on their responsibilities when handling personal information.

Scope

This policy applies to all employees, workers, agency staff, contractors, consultants, volunteers, temporary staff and any other individual who processes personal data on behalf of The ExcluSec Group Ltd.
The policy applies to all personal data regardless of format, including:

- Electronic records.
- Paper records.
- CCTV footage.
- Audio recordings.
- Photographs.
- Email correspondence.
- Mobile devices.
- Cloud-based systems.
- Physical archives.

Data Protection Principles

The ExcluSec Group Ltd will ensure that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date where necessary.
- Retained only for as long as required.
- Processed securely using appropriate technical and organisational measures.
- Managed in a manner that enables the company to demonstrate compliance.

Lawful Basis for Processing

The company will only process personal data where a lawful basis exists.
Depending on the circumstances, processing may be based upon:

- Consent.
- Performance of a contract.
- Compliance with a legal obligation.
- Protection of vital interests.
- Public task.
- Legitimate interests.

Where special category data or criminal offence data is processed, an additional lawful condition under UK GDPR and the Data Protection Act 2018 will also be identified and documented.

Special Category Data
Certain information requires additional protection due to its sensitive nature.
This may include information relating to:
- Health.
- Disability.
- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Trade union membership.
- Sexual orientation.
- Biometric data.
- Criminal convictions and offences.

The company will only process such information where permitted by law and where appropriate safeguards are in place.

Data Collection
Personal information will only be collected where there is a legitimate business, contractual or legal need.

The company will ensure that individuals are provided with clear information explaining:
- Why their information is being collected.
- How it will be used.
- Who it may be shared with.
- How long it will be retained.
- Their rights under data protection legislation.

This information will usually be provided through privacy notices.

Data Security
The ExcluSec Group Ltd is committed to maintaining the confidentiality, integrity and availability of personal information.
Appropriate security measures include:
- Password protection.
- Multi-factor authentication where available.
- Access controls based on business need.
- Secure storage systems.
- Encryption of sensitive data where appropriate.
- Physical security controls.
- Secure disposal arrangements.
- Regular monitoring and review of systems and controls.

Employees must take all reasonable precautions to prevent unauthorised access, disclosure, loss, theft or misuse of personal information.

Data Sharing
Personal information will only be shared where there is a lawful basis to do so.
Information may be shared with:
- Clients.
- Regulatory bodies.
- Government agencies.
- Awarding organisations.
- Professional advisers.
- Service providers.
- Law enforcement agencies.

All data sharing arrangements must be appropriately authorised and, where required, supported by contractual safeguards.

Third-Party Processors
Where external organisations process personal data on behalf of the company, appropriate due diligence will be undertaken before engagement.
The company will ensure that processors:
- Provide sufficient guarantees regarding data protection compliance.
- Implement appropriate security measures.
- Process data only on documented instructions.
- Comply with applicable contractual obligations.

Records of Processing Activities
The company maintains appropriate records of personal data processing activities in accordance with legal requirements and operational needs.
Records may include:
- Categories of personal data processed.
- Categories of individuals.
- Purposes of processing.
- Lawful bases relied upon.
- Data sharing arrangements.
- Retention periods.
- Security measures.

Data Retention and Disposal
Personal information will not be retained for longer than necessary.

Retention periods will be determined by:
- Legal obligations.
- Regulatory requirements.
- Contractual requirements.
- Business needs.
- Industry best practice.

When information is no longer required, it will be securely destroyed, deleted or anonymised.
Further details are contained within the company's Data Retention and Disposal Policy.

Data Subject Rights
Individuals have rights under UK GDPR, including:
- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights relating to automated decision making and profiling.

Requests relating to these rights will be handled promptly and in accordance with legal requirements.

Data Breaches
Any actual or suspected personal data breach must be reported immediately to management.
Examples include:
- Loss of devices or paperwork.
- Unauthorised disclosure of information.
- Cyber security incidents.
- Accidental sharing of personal data.
- Unauthorised access to systems.

All reported incidents will be investigated and appropriate action taken.

Where required by law, breaches will be reported to the Information Commissioner's Office and affected individuals within the relevant statutory timescales.

Data Protection Impact Assessments
The company will undertake Data Protection Impact Assessments where processing is likely to result in a high risk to the rights and freedoms of individuals.

This may include:
• New technologies.
• New surveillance systems.
• Large-scale processing activities.
• High-risk processing involving sensitive information.

Training and Awareness
All employees are responsible for protecting personal information.
The company will provide appropriate data protection and information security training to ensure employees understand:
• Their legal obligations.
• Company procedures.
• Information security requirements.
• Reporting arrangements for incidents and breaches.

Failure to comply with this policy may result in disciplinary action.

Monitoring and Review
The company will regularly review its data protection arrangements to ensure continued compliance with legal, regulatory and operational requirements.

Audits, risk assessments and compliance reviews may be undertaken periodically to identify opportunities for improvement and to ensure the effectiveness of controls.

Responsibilities
All employees are responsible for complying with this policy and protecting the personal information they access, process or manage.

Managers are responsible for ensuring that employees understand and comply with their data protection obligations.

The Compliance Team is responsible for overseeing data protection arrangements, providing guidance, monitoring compliance and supporting the management of data protection risks and incidents.

Failure to comply with this policy may result in disciplinary action and, where appropriate, legal or regulatory action.

Signed: 

Name: Matthew Wellington

Position: Managing Director

Date: 01/04/2026