Policy

1. Purpose

At Excalon Ltd, we are committed to protecting the personal data of all individuals associated with our organisation. This includes employees, contractors, apprentices, consultants, agency workers, and volunteers. We recognise the importance of handling personal data responsibly and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and guidance issued by the Information Commissioner's Office (ICO).

This policy outlines how we collect, use, store, share, and dispose of personal data, and explains your rights and responsibilities under data protection law.

2. Reference documents

- Data Protection Act 2018
- Company vehicle Camera Policy 017

3. Scope of the Policy

This Policy applies to all personal data processed by Excalon Ltd in the context of employment and business operations. It covers:

- Current, former, and prospective employees.
- Contractors, consultants, an agency workers.
- Apprentices and volunteers.
- Any third parties whose data we process in the course of our operations.

4. Policy

Our Role as a Data Controller

Excalon Ltd is a data controller. This means we determine the purposes and means of processing personal data. We are accountable for ensuring that all processing activities comply with the principles and obligations set out in the UK GDPR and the Data Protection Act 2018.

Data Protection Principles

We adhere to the following principles when processing personal data:

1. Lawfulness, fairness, and transparency – We process data lawfully and provide clear information about how it is used.
2. Purpose limitation – Data is collected for specified, explicit, and legitimate purposes.
3. Data minimisation – We only collect data that is adequate, relevant, and limited to what is necessary.
4. Accuracy – We take reasonable steps to ensure data is accurate and kept up to date.
5. Storage limitation – Data is retained only for as long as necessary.
6. Integrity and confidentiality – We implement appropriate security measures to protect data.
7. Accountability – We are responsible for demonstrating compliance with these principles.

Categories or Personal Data We Process

We collect and process various categories of personal data as part of our employment and operational obligations. This may include:

Core Personal Data

- Recruitment and employment details (CVs, applications, interview notes, references).
- Contact and emergency contact information.
- Personal identifiers (e.g. name, date of birth, gender, marital status).
- Employment and contractual information (e.g. job title, hours, salary, benefits).
- Financial and tax-related data (e.g. bank account, NI number, tax code).
- Proof of right to work (e.g. passports, visas, ID cards).
- Disciplinary, grievance, and performance records.
- Training and qualification data.
- Use of company IT systems, CCTV recordings, and photographs.
- Background screening results (e.g. DBS checks, security clearance).

Additional Data (where relevant to the role)

- Health information (e.g. allergies, medical alerts, medications)
- Health and safety training and certification
- Vehicle and driving information
- Photographic ID for site access and security purposes
- System usage audit logs

Where further information is required beyond the above, we will always inform you of what data is being collected, the reasons for its collection, and how it will be used.

We ensure that special category and criminal offence data is processed only under strict conditions and with appropriate safeguards.

Lawful Bases for Processing

We will only process your personal data where we have a lawful reason to do so. These reasons may include:

- Contractual necessity – to fulfil our obligations under your employment or service contract.
- Legal obligation – to comply with legal and regulatory requirements, such as right-to-work checks or HMRC reporting.
- Legitimate interests – for purposes that support our business operations, such as workforce management, security, and infrastructure monitoring, provided these interests are not overridden by your rights.

We routinely review our data processing activities to ensure they remain necessary, proportionate, and legally justified. For higher-risk processing, we may conduct Data Protection Impact Assessments (DPIAs) to evaluate potential impacts on your rights.

For special category data (e.g. health information), we only process this data when a lawful condition applies, such as:

- You have given explicit consent.
- The data is needed for employment or social protection law compliance.
- Processing is necessary to protect vital interests in emergencies.
- You have made the data public
- Processing is required for legal claims or occupational health purposes.

Transparency and individual Rights

We are committed to transparency and provide clear privacy notice explaining how personal data is used. Under UK data protection law, individuals have the right to:

- Be informed about data processing.
- Access their personal data.
- Rectify inaccurate data.
- Erase data (right to be forgotten)
- Restrict or object to processing.
- Data portability.
- Object to automated decision-making and profiling.

Requests can be made by contacting our Data Protection Officer (DPO). We respond within one month, unless an extension is justified.

Data Sharing and Third Parties

We may share data with:

- Internal departments (e.g. HR, IT, Finance)
- External service providers (e.g. payroll, benefits, occupational health).
- Government bodies (e.g. HMRC, Home Office).
- Legal and professional advisors.
- IT and software vendors.

All third parties are subject to Data Processing Agreements (DPAs) and must comply with our data protection standards. We conduct due diligence before engaging any third-party processor.

Data Security Measures

We implement robust technical and organisational measures to protect personal data, including:

- Encrypted systems and secure access controls.
- Two-factor authentication and firewalls.
- Regular audits and access reviews.
- Secure disposal of data (digital and physical).
- Firewalls, antivirus software, VPNs, and encrypted communications
- Staff training and awareness programmes.

Personal data must not be stored on personal devices or removed from company premises without authorisation.

Data Retention

We retain personal data only as long as necessary, in line with our Data Retention Policy:

- Employment records: 1-year post-employment.
- Payroll / tax data: Up to 6 years.
- DBS checks: Deleted within 6 months unless legally required for longer.

Retention periods are reviewed regularly, and data is securely deleted or anonymised when no longer needed.

Data Breaches

All data breaches must be reported immediately to the DPO. We investigate and document all incidents. If a breach poses a risk to individual's rights, we notify the ICO within 72 hours and inform affected individuals without undue delay.

Monitoring and Surveillance

We may monitor IT systems, emails, internet usage, and CCTV for legitimate business purposes, including:

- Ensuring compliance with company policies.
- Protecting company assets.
- Investigating misconduct.
- Ensuring health and safety.

Monitoring is proportionate, transparent, and subject to data protection safeguards.

Responsibilities of Staff and Associates

All staff and associates must:

- Comply with this policy and related procedures.
- Access personal data only when authorised and necessary.
- Report any suspected data breaches.
- Complete mandatory data protection training.

Non-compliance may result in disciplinary action, including termination of employment or contract.

Contact and Further Information

For questions, concerns, or to exercise your data rights, contact:

Data Protection Officer Excalon Ltd –

Sarah Dyson - sarah.dyson@excalon.com - 07501 743 798

You may also contact the Information Commissioners Office (ICO) at www.ico.org.uk or call 0303 123 1113.

5. Records Management

All employees must maintain all records relevant to administering this process and procedure in line with Legislation and the Company record keeping system.

6. Policy Review

The Company will monitor its policies, processes and procedures to implement changes to improve them and ensure that they comply with best practice, legislation changes and the emerging marketplace.

VERSION HISTORY			
Document Version	**Version Date**	**Revision Description**	**Author**
0.1		Initial	

APPROVALS			
Document Version	**Version Date**	**Approver Name & Title**	**Signature**
0.1	24-9-25	K. O'DONNELL.	

DISTIRUBITON LIST		
Name	**Role**	**Location**
All Employees	Company Wide	All Offices