Data Protection Policy

1. POLICY STATEMENT

Datalink Electronics Ltd is committed to ensuring that personal data is processed lawfully, fairly and transparently and is protected from unauthorised access, loss, misuse or disclosure.

The Company will implement appropriate technical and organisational measures to safeguard personal data and ensure compliance with all applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. PURPOSE

The purpose of this policy is to:

- Set out Datalink Electronics Ltd.'s commitment to protecting personal data
- Ensure compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Establish clear principles for the collection, handling, storage, retention, and protection of personal data

3. SCOPE

This policy applies to:

- All employees, including Directors and Managers
- Contractors, suppliers and third parties acting on behalf of the Company
- All personal data processed by the Company, regardless of format (electronic or paper)

Personal data includes any information relating to an identified or identifiable individual, including but not limited to names, contact details, identification data, and online identifiers.

4. LAWFUL BASIS FOR PROCESSING

Personal data will only be processed where there is a lawful basis to do so under UK GDPR. These may include:

- Consent
- Performance of a contract
- Compliance with a legal obligation
- Protection of vital interests
- Performance of a task conducted in the public interest
- Legitimate interests of the Company, where these are not overridden by individuals' rights

The lawful basis relied upon will be documented where required.

5. DATA PROTECTION PRINCIPLES

Datalink Electronics Ltd adheres to the principles of UK GDPR. Personal data shall be:

- 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
- Retained only for as long as necessary
- Processed securely to maintain confidentiality and integrity
- Processed in line with individuals' rights

6. RESPONSIBILITIES

- The Managing Director has overall responsibility for ensuring compliance with this policy.
- All employees must manage personal data in accordance with this policy, complete required data protection training, and report any data breaches or concerns immediately.
- Managers must ensure effective implementation of this policy, promote data protection awareness, and monitor compliance within their teams.
- IT must ensure systems and security controls are effective, and maintain secure data storage, backups, and access controls.
- The Data Protection Lead must monitor compliance and advise on data protection obligations, handle data subject rights requests, review data protection policies and procedures, and oversee Data Protection Impact Assessments (DPIAs) where required.

7. DATA PROTECTION RISKS

The Company recognises key risks including:

- Unauthorised access or disclosure of personal data
- Data loss or corruption
- Failure to meet legal obligations
- Reputational damage resulting from data breaches

Appropriate technical and organisational controls are implemented to mitigate these risks.

8. DATA STORAGE AND SECURITY

Datalink Electronics Ltd ensures that:

- Personal data is stored securely, whether electronically or in paper format
- Access is restricted to authorised personnel on a need-to-know basis
- Strong passwords, access controls, and encryption are used where appropriate
- Security software and systems are maintained and updated
- Paper records are stored securely and disposed of safely
- Regular backups are maintained and tested

Personal data must not be stored on unauthorised devices or systems.

9. DATA USE AND HANDLING

When handling personal data, employees must:

- Only access data necessary for their role
- Not share data informally or with unauthorised individuals
- Keep systems and devices secure when unattended
- Avoid transferring data outside approved systems

10. DATA ACCURACY AND RETENTION

The Company will:

- Take reasonable steps to ensure personal data is accurate and up to date
- Correct or delete inaccurate data promptly
- Retain personal data only in line with the Company's Data Retention Schedule
- Securely dispose of personal data once retention periods expire

11. DATA SUBJECT RIGHTS

Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request erasure where appropriate
- Restrict or object to processing
- Be informed about how their data is used

All requests will be handled in accordance with statutory timeframes.

12. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

Where processing activities are likely to result in a high risk to individuals' rights and freedoms, the Company will conduct a Data Protection Impact Assessment prior to processing.

13. REPORTING DATA BREACHES

All actual or suspected data breaches must be reported immediately. The Company will:

- Investigate incidents promptly
- Take corrective action where necessary
- Report breaches to the Information Commissioner's Office (ICO), where legally required

14. TRAINING AND AWARENESS

All employees will receive data protection training appropriate to their role. Refresher training will be provided periodically to ensure ongoing compliance.

15. MONITORING AND REVIEW

This policy will be reviewed annually and updated as necessary to reflect changes in legislation, regulatory guidance, or business operations.

NAME:	Mariam Smith	**SIGNED:**	Mariam Smith
POSITION:	Managing Director	**DATE:**	01/04/2026