



Data Protection Policy Statement

Datalink Electronics Ltd needs to gather data and use certain information about individuals. These can include Customers, Suppliers, employees and other people the Company has a relationship with or needs to contact. The policy describes how personal data must be collected, handled and stored to meet Data Protection standards and comply with the law.

Definition

This Data Protection Policy Statement ensures Datalink Electronics Ltd:

- Complies with the Data Protection law and follows good practice.
- Protects the rights of staff, Customers and partners.
- Is open about how it stores and processes individual's data.
- Protects itself from the risks of a data breach.

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically or on paper. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights for data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Scope

This policy applies to the head office of Datalink Electronics Ltd; all staff and volunteers of Datalink Electronics Ltd; and all contractors, suppliers and other people working on behalf of Datalink Electronics Ltd.

It applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside the Data Protection Act 1998. This can include names of individuals, postal addresses, email addresses, telephone numbers, plus any other information relating to individuals.

Data Protection Risks

The policy helps to protect Datalink Electronics Ltd from real data security risks, including:

- **Breaches of confidentiality:** information being given out inappropriately.
- **Failing to offer choice:** all individuals should be free to choose how the Company uses data relating to them.
- **Reputational damage:** the Company could suffer if hackers successfully gained access to sensitive data.





Responsibilities

Everyone who works for or with Datalink Electronics Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- Directors are ultimately responsible for ensuring Datalink Electronics Ltd meets its legal obligations.
- The Data Protection Officer, Mariam Smith, is responsible for:
 - Keeping the board updated about Data Protection responsibilities, risks and issues
 - Reviewing all Data Protection procedures and related policies, in line with an agreed schedule
 - Arranging Data Protection training and advice for the people covered by this policy
 - Handling Data Protection questions from employees and anyone else covered by this policy
 - Dealing with requests from individuals to see the data held about them ('subject access request')
 - Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive information
 - Approving any Data Protection statements attached to communications such as emails/letters
 - Addressing any Data Protection queries from journalists or media outlets like newspapers
 - Working with other employees to ensure marketing initiatives abide by Data Protection principles
- IT Officer, Michael Belcher, is responsible for:
 - Ensuring systems, services and equipment used for storing data meet acceptable security standards
 - Performing regular checks/scans to ensure security hardware and software is functioning properly
 - Evaluating any third-party services the Company is considering using to store or process data

General Employee Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers
- Datalink Electronics Ltd will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure by taking sensible precautions and following guidelines
- Strong passwords must be used and should never be shared
- Personal data should not be disclosed to unauthorised people, either internal or external
- Data should be regularly reviewed and updated if it is found to be out of date; if no longer required, it should be deleted and disposed of
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of Data Protection

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager (Michael Belcher) or Data Protection Officer (Mariam Smith).

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper, and printouts are not left where unauthorised people could see them
- Data printouts should be shredded and disposed of securely when no longer required





When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared
- If data is stored on removeable media, these should be kept locked away when not being used
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service
- Servers containing personal data should be sited in a secure location, away from the general office
- Data should be backed up frequently, and those backups tested regularly, in line with the Company's standard backup procedures
- Data should never be saved directly onto laptops or other mobile devices like tablets or smartphones
- All servers and computers containing data should be protected by approved security software and firewall

Data Use

Personal data is of no value to Datalink Electronics Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are locked when left unattended
- Personal data should not be shared informally and never sent by email, as this is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers and must always access and update the central copy of any data

Data Accuracy

The law requires Datalink Electronics Ltd to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Datalink Electronics Ltd should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as possible and no unnecessary additional data sets will be created
- Employees should take every opportunity to ensure data is updated i.e. by confirming a Customer's details when they call
- Datalink Electronics Ltd will make it easy for data subjects to update the information that is held about them i.e. via the company website
- Data should be updated as inaccuracies are discovered i.e. if a Customer can no longer be reached by their stored telephone number, it should be removed from the database

Subject Access Request

All individuals who are the subject of personal data held by Datalink Electronics Ltd, are entitled to:

- Ask what information the Company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the Company is meeting its Data Protection obligations





If an individual contacts the Company requesting this information, this is called a Subject Access Request. They should be made aware by email, address to the Data Controller (msmith@datalink-electronics.co.uk). The Data Controller can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per Subject Access Request. The Data Controller will aim to provide the relevant data within 14 days and will always verify the identity of anyone making the request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Datalink Electronics Ltd will disclose the requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the Board and from the Company's legal adviser where necessary.

Providing Information

Datalink Electronics Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights.

To these ends, the Company has a privacy statement, setting out how data relating to individuals is used by the Company. This is available on request, or you can download a version from Datalink's website.

This Data Protection Policy Statement will be reviewed for each financial year and revised as necessary to reflect changes to the business activities and any changes to legislation. Any changes to the Policy will be brought to the attention of all employees.

NAME: Mariam Smith

SIGNED: *Mariam Smith*

POSITION: Managing Director

DATE: 01/04/2025

