Data Protection Policy

Introduction

Larkshill Engineering Limited needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

This policy should be read in conjunction with the company's Information and Cyber Security Policy: *Infocybersecuritypolicy001*.

Why this policy exists

This data protection policy ensures Larkshill Engineering Limited:

- complies with data protection law
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulation (GDPR) describe how organisations, including Larkshill Engineering Limited, must collect, handle, use and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. 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 of 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

Policy scope

This policy applies to:

- All sites of Larkshill Engineering Limited
- All employees of Larkshill Engineering Limited
- All contractors, suppliers and other people working on behalf of Larkshill Engineering Limited

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of The Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulation (GDPR). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect Larkshill Engineering Limited from some very real data security risks, including:

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

Responsibilities

Everyone who works for or with Larkshill Engineering Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Every employee that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.

• 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.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller. 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 out for some reason:
• 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, like on a printer.
• 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 between employees. Larkshill Engineering's 'Information and Cyber Security Policy', document re. Infocybersecuritypolicy001, details the password policy rules (see below):

All passwords must, where the software, computer, or device allows:

a. made up of 3 random words and include a number and symbol
b. be at least 12 characters;
c. cannot be the same as the previous 10 passwords you have used;
d. not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of Senior Management who will liaise with the IT Lead/s as appropriate and necessary.

• If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
• Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
• Servers containing personal data should be sited in a secure location, away from general office space.
• Data should be backed up frequently, those backups should be tested regularly, in line with the company's standard backup procedures.
• Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
• All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Larkshill Engineering Limited 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 always locked when left unattended.
• Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication 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. Always access and update the central copy of any data.

Data accuracy
The law requires Larkshill Engineering Limited 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 Larkshill Engineering Limited 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 necessary. Staff should not create any unnecessary additional data sets.

• Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
• Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

All individuals who are the subject of personal data held by Larkshill Engineering Limited 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. Subject access requests from individuals should be made by email, addressed to the data controller at gaynor@larkshill.com. The data controller will aim to provide the relevant data within 14 days but no longer than one month from the date of request.

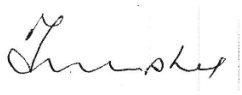
The data controller will always verify the identity of anyone making a subject access request before handing over any information. In certain circumstances, The Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulation (GDPR) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Larkshill Engineering Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from senior management and from the company's legal advisers where necessary.

Larkshill Engineering Limited aims to ensure that individuals are aware that their data is being processed, and that they understand:

• How the data is being used
• How to exercise their rights

To these ends, the company has a privacy statement, Document: *Data Privacy Policy 001*, setting out how data relating to individuals is used by the company.

In addition, the company has an Information and Cyber Security Policy: *Infocybersecuritypolicy001*, setting out the company's required security measures for all the information it holds to ensure the highest standards of information security.



Frank Murphy

Managing Director