LIGHT PROJECTS

Data Security Policy

Introduction

Light Projects Ltd 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.

Why this policy exists

This data protection policy ensures that the Company:

- Complies with data protection law and follow good practice
- 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

Policy scope

This policy applies to all staff, suppliers, contractors and people working on behalf of Light Projects Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR rules. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

…plus any other information relating to individuals

Data protection risks

This policy helps to protect Light Projects Ltd 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 Light Projects 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:

The board of directors is ultimately responsible for ensuring that the Company meets its legal obligations.

The data co-ordinator 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 staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Light Projects Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The IT manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and 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. For instance, cloud computing services.

The marketing manager is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff 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.
- Light Projects 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 the guidelines below.
- In particular, strong passwords must be used and they should never be shared.

Registered office: 146 High Street Billericay CM12 9DF • Registered in England number 01893557 • VAT Number GB 429 5437 30

• 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.

• Employees should request help from their line manager or the data co-ordinator if they are unsure about any aspect of data protection.

Data Storage and Use

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or 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.

• Any documents scanned on the networked photocopier should not be saved in the internal memory of the machine.

• 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. Strong passwords should be made of a series of letters (upper and lower case), numbers, and symbols

• If data is stored on removable media (like a CD / DVD / USB thumb drives), then these should be kept locked away securely when not being used.

• Data should only be stored on designated drives and servers.

• Servers containing personal data should be sited in a secure location.

• Company wireless networks should be secured using strong passwords, with the said passwords being made available to designated staff members only.

• Access to company databases should be apportioned on a restricted basis to prevent the accidental deletion of data.

• Mobile telephones should be protected with a password / pin.

• Email clients on all Computers and Phones should be protected by strong passwords.

• Any internal mails that contain personal data should be encrypted.

• Emails that contain personal data and need to be transmitted externally should have their contents

contained inside a Microsoft Word document with a strong password. The said password should be communicated to the recipient via another method, such as text message.

• Access to the company email / database servers should only be made over a secure (SSL) connection from mobile telephones / web browsers or via IBM Notes clients.

• All VPN users should utilise strong passwords when accessing the company network.

• 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 PC's, laptops or other mobile devices like tablets or smart phones.

• Data should always be accessed and updated centrally.

• All servers and computers containing data should be protected by approved security software and a firewall.

• Logons to servers should be audited to detect any unauthorised access.

• Users should always lock their workstation when away from their desks.

January 2020

-ends-