LEIGHTON HALL

DATA PROTECTION POLICY

CONTEXT AND OVERVIEW

Policy prepared by: Lucy Arthurs, Estate Manager / Data Protection Officer
Policy became operational on: 25th May 2018
Review Date: 25th May 2020

Introduction

Leighton Hall needs to gather and use certain personal information data about individuals.

These can include customers, suppliers, business contact, employees, as well as other 3rd parties and people that the company 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 new General Data Protect Regulation standards (GDPR), to comply with this new European Law.

Why this policy exists

This Data Protection Policy ensures that Leighton Hall:-

- Complies with the new GDPR Law
- Has good procedures in place
- Practices and reviews its procedures
- Protects the rights of Employees, Customers and Business Partners
- Is open about how is collects, handles, processes and stores individuals' data
- Protects itself from the risk of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations, including Leighton Hall collect, handle 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:-

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

Leighton Hall, Carnforth, Lancashire, LA5 9ST **T.** 01524 734474 **E.** info@leightonhall.co.uk **www.leightonhall.co.uk**

PEOPLE, RISK AND RESPONSIBILITIES

Policy Scope

This policy applies to:

- All partners, staff and any volunteers of Leighton Hall
- All contractors, suppliers and any 3rd parties working on behalf of Leighton Hall

It applies to all data that Leighton Hall holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:-

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Financial details and references
- Employees information i.e. PAYE, Pension

Data Protection Risk

The policy helps to protect Leighton Hall from some 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 gain access to sensitive data

Responsibilities

Everyone that works for or with Leighton Hall has some responsibility for ensuring data is collected, handled, used and stored appropriately.

Every employee – full time, seasonal or voluntary – that handles personal data must ensure that it is handled and processed in line with this policy and the Data Protection Procedure attached.

However, these people have key areas of responsibility:

- The partners of Leighton Hall are ultimately responsible for ensuring that Leighton Hall meets its legal obligations
- The Data Protection Officer, Lucy Arthurs, is responsible for:-
    - Keeping the Partners and all employees updated about data protection responsibilities, risk and any other issues.
    - Reviewing all data protection procedures and related policies, in line with a schedule.
    - Arranging data protection training and advice for the employees covered by this policy, if requested.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Leighton Hall holds about them. This is known as "Subject Access Requests".
    - Arranging where required, checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The Data Protection Officer will work with an external 3rd party IT Manager – Barry Morgan – to be 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 i.e. cloud company services.

Leighton Hall, Carnforth, Lancashire, LA5 9ST **T.** 01524 734474 **E.** info@leightonhall.co.uk **www.leightonhall.co.uk**

- The Data Protection Officer will work with an external 3rd party Marketing & PR Manager – Kate Bowyer - to be responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from the media outlets such as 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 either Lucy Arthurs, Data Protection Officer or one of the partners.
- L**eighton Hall 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 follow the guidelines below.
- **Strong passwords must be used**, and they should not be shared.
- Personal data **should not be disclosed** to unauthorized 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 Lucy Arthurs, 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 Lucy Arthurs, Data Protection Officer, and if she doesn't have the answer she can work with the external 3rd party IT Manager – Barry Morgan, to find the answer.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people, such as the general public, cannot see it: i.e. one of our offices.

These guidelines also apply to data that is usually stored electronically, but has been printed off for some reason:

- When not required, the paper or file should be **kept in a locked drawer or filing cabinet**. The office in the basement at Leighton Hall is to be locked whenever it is empty.
- 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.
- 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 company service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should **never be saved directly** onto laptops or other mobile devices like tables or smart phones.
- Data should be **backed up frequently**. Those backups should be tested regularly.
- All servers and computers containing data should be protected by **approved security software and a firewall i.e. ESET**

Leighton Hall, Carnforth, Lancashire, LA5 9ST **T.** 01524 734474 **E.** info@leightonhall.co.uk **www.leightonhall.co.uk**

Data Use

Personal data is of no value to Leighton Hall unless the business can make use of it. However, it is when personal data is accessed and used that it can be 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** i.e. by email. At Leighton Hall we use Microsoft Outlook as our email system, and we have switched on the encryption mode, therefore all our emails are automatically encrypted in transmission.
- 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 on the network.

Data Accuracy

The law requires Leighton Hall to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that personal data is accurate, the greater the effort Leighton Hall 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 or copies.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Leighton Hall will make it **easy for data subjects to update the information** Leighton Hall holds about them. See our Privacy Notice.
- Data should be **updated as inaccuracies are discovered**.

Subject Access Requests

All individuals who are the subject of personal data held by Leighton Hall, including employees, are entitled to:-

- Ask **what information** Leighton Hall holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how Leighton Hall is **meeting its data protection obligations**.

If an individual contacts Leighton Hall requesting this information, this is called a "Subject Access Request".

Subject Access requests from individuals should be made by email or letter addressed to the Data Controller at info@leightonhall.co.uk or FTO Data Controller, Leighton Hall, Carnforth, Lancashire, LA5 9ST.

The Data Controller will always try and verify the identity of anyone making a Subject Access Request before handing over any information, but will aim to provide the relevant data within 14 days.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Leighton Hall will disclose requested data. However, the Data Controller will ensure the request is legitimate, seek assistance from the Leighton Hall Partners and from our legal advisers where necessary.

Leighton Hall, Carnforth, Lancashire, LA5 9ST **T.** 01524 734474 **E.** info@leightonhall.co.uk **www.leightonhall.co.uk**

Providing Information

Leighton Hall 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, Leighton Hall has a Privacy Notice, setting out how data relating to individuals is used. This notice is available on request or it can be downloaded from our website – www.leightonhall.co.uk

Data Breaches and What to do if a Breach is Discovered?

What is a Data Breach?

All staff must understand what a Data Breach is:-

- Data has been sent to the wrong recipient either by email or post
- Theft
- Data collection hardware has been lost by a member of staff i.e. a USB stick left on the bus

What to do if there is a Data Breach?

If any member of staff believes they have identified a Data Breach as listed above, they must:-

- Make the Data Protection Officer and / or the Partners aware immediately
- Identify what and where the data breach is and when it happened.
- Try and rectify the issues with the IT Manager
- Call the Information Commissioner Office (IOC)– they are the body that is tasked with enforcing the GDPR Law in the UK:- Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF - Telephone 0303 123 1113 - https://ico.org.uk/concerns/

Leighton Hall, Carnforth, Lancashire, LA5 9ST **T.** 01524 734474 **E.** info@leightonhall.co.uk **www.leightonhall.co.uk**