Data Protection Policy

Issue Date:
May 2018

Review Date:
May 2019

Prepared by:
The Chichester Hotel
Replaces:

This policy is an update of the policy prepared in 2013 and with a view to complying with GDPR which is effective 25th May 2018.

Overview:
The Company is committed to ensuring that all data held by it is processed in accordance with the Data Protection Regulations and or any other rules or legal obligations imposed upon the Company.

The Company as part of its activities needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people 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 Company's Data Protection obligations and to comply with the law.

Training implications:
General principles to be covered by line managers at local induction.

Foreword

Please note any reference to employees contained within this document also applies to partners.

Why this Policy Exists

This Data Protection policy ensures that this company:

- Complies with Data Protection law and follows good practice;
- Protects the right of staff, customers, business contacts, suppliers and partners;
- Is open about how it stores and processes the data of individuals;
- Protects itself from the risk of a data breach.

Data Protection

This Company understands that to comply with the law, information including personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Company's obligations are underpinned by a number of important principles. These say that information, including personal information, 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 any longer than necessary;
- be protected in appropriate ways thus ensuring an adequate level of protection.

Policy Scope

This Policy applies to this organisation as a whole including its various sites and venues, associated companies, all staff and volunteers and all contractors, suppliers working on behalf of this Company.

It applies to all data which the Company holds relating to identifiable individuals and can include:-

- names of individuals;
- email addresses;
- telephone numbers;
- your home address and contact details;
- recruitment records and references;
- bank details;
- appraisals and performance records;
- sickness records;
- salary bonuses and other benefits; and
- records of telephone use;
- plus any other information relating to individuals.

This list is intended as a guide and is not exhaustive.

The Company is required to take steps to ensure that data is kept accurate and up to date. It is the responsibility of all employees to take reasonable steps and not to create additional unnecessary data. Staff should take every opportunity to ensure that data is updated for instance by confirming a customers or employees details when the opportunity arises. Data should be updated from time to time. It is the Company's responsibility to ensure marketing data bases are checked against industry suppression files every six months.

Data Protection Risks

This Policy helps to protect this company from 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.

Key Individuals

Everyone who works for this organisation has some responsibility for ensuring data is collected, stored and handled appropriately. All individuals who handle personal data must make sure that it is handled and processed in line with this policy and data protection principles.

The Board of Directors are ultimately responsible for insuring that this company meets its legal obligations.

The Chichester Hotel 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;
- handling Data Protection questions from staff and anyone else covered by this policy;
- dealing with Subject Access Requests.

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 accessed 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 appropriate guidelines;
- 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 HR Department/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 draw or filing cabinet. Employees should make sure that paper and printouts are not left where unauthorised people could see them, like on a printer. Data should be shredded and disposed of securely when no longer required.

Electronically stored data must be protected from unauthorised access, accidental deletion and malicious hacking attempts. Strong passwords should be used, which are changed regularly and never shared. Data stored on removal media, like a cd or dvd, should be kept locked away securely when not being used.

Data should only be stored on designated drives or servers and should only be uploaded to an approved cloud computing service. Servers containing personal data should be cited in a secure location and data should be backed up frequently. Back up data should be tested regularly in line with standard back up procedures. It is advisable not to save data directly to laptops or other mobile devices like tablets or smart phones. Approved security software and a firewall should be used to protect data.

Subject Access Requests

All individuals who are the subject of data held by this organisation are entitled to ask what information the Company holds about them and why. They can ask how to gain access to it and be informed as to how to keep it up to date. They are also entitled to be informed as to how the Company is meeting its Data Protection obligations.

The individual is required to notify the Company promptly of any changes in their personal information, which they become aware of and which is held by the Company, for example, contact details, bank details, marital status or criminal convictions.

Individuals may be charged £10.00 per Subject Access Request. The Company will aim to respond to all requests within 21 days. There may, however, be circumstances in which the Company cannot release information to you, for example, where it contains personal data

about another employee or third party. All requests will be verified before the information is provided.

The Company takes all reasonable steps to keep your information confidential and will not disclose your personal information to anyone outside of the Company. However, the Company may do so if it is required for the administration of your employment and associated benefits (e.g. in relation to pension providers or administration of insurance schemes).

The Company may also need to make your information available to its professional advisers (e.g. lawyers, accountants) or legal and regulatory authorities (e.g. Revenue and Customs).

The Company has a Privacy Notice available on its website which sets out how data relating to individuals is used by the Company. A version of this statement is also available on the same website.