Maesycwmmer, Nr Ystrad Mynach, Caerphilly, CF82 7SN
01495 225590 www.brynmeadows.co.uk

DATA POLICY

Introduction

Bryn Meadows Golf and Country Club Ltd known as Bryn Meadows Golf Hotel & Spa needs to gather information and use certain information about individuals. These can include suppliers, customers, 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, stored and used to meet the company's data protection standards and to comply with the law.

Why This Policy Exists

The data protection policy ensures Bryn Meadows Golf Hotel & Spa:

- 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 the company, Bryn Meadows Golf Hotel & Spa, all staff and volunteers of the company, all contractors, suppliers, other people working on behalf of the company and customers. 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 1998. This can include:

- Names of individuals
- Postal or billing addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data Protection Law

The Data Protection Act 1998 describes how organisations, including Bryn Meadows Golf Hotel & Spa must 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 important principles and lawful basis for processing. These say that personal data must:

1. Consent, to be processed fairly and lawfully
2. Performance of a contract
3. Compliance with a legal obligation
4. Necessary to protect the vital interests of a data subject
5. Necessary for the performance of task carried out in the public interest
6. Necessary for the purpose of legitimate interests

Contractually, data is required to be lawfully kept for 7 years for reporting or legal purposes such as governed regulations including VAT records. However data may be stored for longer periods than

this. Individual or personal data can be requested to be deleted or destroyed, including hard copies and back-ups, as long as it does not need to be legitimately or lawfully kept.

Responsibilities

Everyone who works for or with Bryn Meadows Golf Hotel & Spa 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 the policy and data protection principles.

However, these people have key areas of responsibility:

- The Director(s) is/are ultimately responsible for ensuring that Bryn Meadows Golf Hotel & Spa meet its legal obligations
- The Data Protection Officer, Gavyn Bolton, General Manager, is responsible for:
    - Keeping the director(s) updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in link with 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 Bryn Meadows Golf Hotel & Spa holds about them (Subject Access Requests).
    - Checking the approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The IT Manager, Sabre Computer & IT Services Ltd, 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, Cerys John, is responsible:
    - 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. All of our systems are password protected, and all activity can be logged and tracked by users.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their managers.
- Bryn Meadows Golf Hotel & Spa 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.
- 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 a data protection officer if they are unsure about any aspect of data protection.

Data Use

Personal data is of no value to Bryn Meadows Golf Hotel & Spa 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 screens of their computer are always locked when unattended.
- Personal data should not be shared informally.
- Data must be encrypted before transferring electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their personal computers.

Data Accuracy

The law requires Bryn Meadows Golf Hotel & Spa and its employees to take reasonable steps to ensure data is kept accurate and up to date.

- 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.
- Bryn Meadows Golf Hotel & Spa will make it easy for data subjects to update the information Bryn Meadows Golf Hotel & Spa holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if they customer can no longer be reached on their stored telephone number, or email address, it should be removed from the database.
- It is the Marketing Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Data Storage

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it. Paper or files are kept in a lockable drawer or filing cabinet, or behind a door that is lockable. Employees should make sure paper and printouts are not left where unauthorised people could see them. Data print outs should be disposed of securely when no longer required.

When data is stored electronically, are to be protected from unauthorised access, accidental deletion and malicious hacking attempts. Employees will protect data by using strong passwords that are changed regularly and never shared between employees. Anything stored on removable media (CD, DVD, USB, etc) are to be kept locked away when they are not being used. Data is stored on designated drives and servers and only uploaded to approved computing services. These are sited in a secure location, away from office space. Data is backed up frequently, and is tested

regularly in accordance with Bryn Meadows Golf Hotel & Spa's standard backup procedures. These will be protected by approved security software and a firewall. Only approved laptops and mobile devices will save data directly.

Data Protection Risks

This policy helps to protect Bryn Meadows Golf Hotel & Spa 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 gain access to sensitive data.

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Any individual who accesses, uses or manages the resorts information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer. If the breach occurs or is discovered outside of normal office working hours (Monday – Friday, 8am-5pm), it must be reported as soon as is practicable. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

The Data Protection Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment will be made by the Data Protection Officer with any other relevant officers appointed to establish the severity of the breach and who will take the lead investigating the breach. It will be established whether there is anything that can be done to recover any losses and limit the damage the breach could cause. It will be established who may need to be notified as part of the initial containment and will inform the police, where appropriate. Advice from experts may be sought in resolving the incident promptly. A suitable course of action to be taken to ensure a resolution to the incident.

Notification will be assessed on a case by case basis; however, the following will need to be considered including whether there are any legal/contractual notification requirements, whether notification would assist the individual affected – could they act on the information to mitigate risks? Whether notification would help prevent the unauthorised or unlawful use of personal data? Would notification help the resort meet its obligations under the seventh data protection principle? If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks.

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, Bryn Meadows Golf Hotel & Spa will disclose requested data. However the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

Privacy and Electronic Communications Regulations (PECR) including Direct Marketing

This sits alongside the Data Protection Act to give people specific privacy rights in relation to electronic communications. The organisation promotes good practice, advice and guidance. This includes rules on:

- Marketing calls, emails, texts, faxes, video messaging, and internet messaging
- Cookies (and similar technologies)
- Keeping communications services secure
- Customer privacy as regards to traffic and location data, itemised billing, line identification and directory listings.

You can be classes as an 'individual subscriber' which covers individual customers (including sole traders) and other organisations and partnerships, or a 'corporate subscriber' which covers subscribers that are a corporate body with separate legal status. This includes companies, limited liability partnerships, and some government bodies and can cover an individual working for a corporate subscriber. Corporate subscribers do not need consent of the individual to contact them.

At Bryn Meadows Golf Hotel & Spa we send out regular email marketing campaigns. Subscription to these are through prize draws, on our website and membership. Guests staying overnight or if you have made a booking with us, and if you have given permission to be contacted directly by a member of staff, this includes enquiries. Please be aware you can be removed from these lists or unsubscribe at any time, following the instructions provided or by contacting the resort. You will not be re-inserted to this list unless you ask to do so in writing. Other forms of marketing could include direct text messages, telephone calls, internet and social media messaging or direct mail. The campaigns are created internally and we do not sell your data onto 3rd parties.

Where we receive personal data from a customer or potential customers, including business cards, in order to provide goods or services, and for legitimate interests of the business, you may be contacted directly by a member of staff including email, telephone calls, text messages, direct mail or internet messaging. The processing activity is undertaken where the lawful basis is that it is for the performance of a contract or with the view of entering into a contract or an informal agreement.

Privacy Notice

When processing personal data guests are provided with a Privacy Notice that sets out among other things the purpose of processing. This will be on the email confirmation, contracted terms, staff handbook and conditions. It is also available on the Bryn Meadows Golf Hotel website, and is also available on request by contacting the resort.

Privacy Policy

This is an internal compliance document for staff at Bryn Meadows Golf Hotel & Spa. It is to be included in the Staff Handbook, and sets out how staff comply with Data Protection and GDPR.

Maesycwmmer, Nr Ystrad Mynach, Caerphilly, CF82 7SN
01495 225590 www.brynmeadows.co.uk

Subject Access Requests

All individuals who are the subject of personal data held by Bryn Meadows Golf Hotel & Spa are entitled to ask what information the company holds about them and why. The Subject Access Request must be received in writing, and will be acknowledged within 7 working days, addressed to the Data Protection Officer. The information provided within 40 calendar days of receiving it. This can be extended by a further 60 days where requests are complex or numerous. The individual will be informed within 30 days of the receipt of request and explain why the extension is necessary. If a disabled person finds it impossible or unreasonably difficult to make a request in writing, a reasonable adjustment will be made for them under the Equality Act 2010.

A copy of the information will be provided free of charge. However, you can be charged a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee can also be charged for further copies of the same information. The fee must be based on the administrative costs of providing the information.

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. The subject access provides a right to see the information contained in personal data, rather than the right to see the documents that include that information.

Information will be provided in English. The act requires us to respond in a an intelligible form, and does not require to be translated. For those whose English comprehension skills are poor, we will try to help you understand our response to the best of our ability.

Providing Information

Bryn Meadows Golf Hotel & Spa 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, setting out how data relating to individuals is used by the company.