Cheshire Golf Limited

DATA PROTECTION POLICY

Introduction

This policy sets out how Cheshire Golf Limited (hereafter known as CGL) processes the personal data of data subjects, including the personal data of job applicants and the personal data of our current and former directors, employees, volunteers, contractors, consultants, members, players, suppliers and other third parties. It applies to all personal data that we process, regardless of the media on which those personal data are stored, e.g., electronically, on paper or on other materials.

The CGL is committed to being clear and transparent about how we collect and use personal data and to complying with our data protection obligations. Protecting the confidentiality, security, and integrity of the personal data that we process is also of paramount importance to our operations.

The CGL will process personal data relating to you in accordance with this policy, the data protection legislation and our current privacy notice which can be found on our website. The Company processes individual personal data in nearly all of our activities. This includes data about employees, volunteers, players, members, website, Instagram, Facebook /app users and more. We consider the impact of data protection legislation on how we handle information that we hold that could be used to identify a living individual such as contact details sent in via email, competition entries sent via a website or transaction details recorded for payment of entry to competitions.

Responsibility

The data controller is CGL Ltd. The contact is the County Secretary whose contact details are **secretary@cheshiregolf.org.uk**

Purpose of Policy

The overall purpose of our processing is for administration of the activities expected of Cheshire Golf Limited, its board and committees. The Policy is designed to ensure you are aware of the legal requirements imposed on you and to give practical guidance on how to comply with them. The Policy also sets out the consequences of failure to comply with them.

Data Protection Laws

The Data Protection Act 2018 (DPA) and General Data Protection Regulations (GDPR) 2018 applies to any personal data that we process.

The Data Protection Laws require that personal data is processed in accordance with the Data Protection Principles and gives individuals rights to access, correct and control how we use their personal data.

In summary the Data Protection Laws require CGL to:

- Only process personal data for certain purposes.
- Process personal data in accordance with the 6 principles of ‘good information handling.

- Provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice. CGL Privacy notice can be found on our website.
- Respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them).
- Keep accurate records of how data is processed and where necessary notify the ICO and possible data subjects when there has been a data breach.

Lawful Basis for Processing Data

For data to be processed lawfully we must be processing it on one of the legal grounds set out in the Data protection Laws.

For the processing of ordinary personal data in our organisation these may include amongst other things.

- Giving consent to the processing, e.g. when registering on the clubs website, or applying for competitions**.** We will not always need consent to process personal data under the GDPR (December 2023). Consent is one way of lawfully processing personal data but is not suitable for all situations. Under the GDPR consent can always be withdrawn, so it is important that you assess carefully whether you do need to rely on consent, or whether there is a more appropriate lawful basis for processing.
- **Example**: We may be required to disclose information regarding golfers to England Golf. This would not require the consent of the individuals as England Golf has a legitimate interest in receiving handicap information, which will typically outweigh an individual's privacy interests regarding handicap information. Where these grounds apply, consent would not be required. What you are required to do is to tell individuals about the disclosure and the reasons behind it. Whatever lawful basis you plan to rely on, you will need to tell individuals your justification for processing their personal data, so documenting this, and communicating it, is important.
- Processing necessary for legal obligations such as company accounts and dealing with tax authorities.
- Necessary for the legitimate interest reasons of the data controller or a third-party e.g. keeping in touch with members, players, participants about competition dates or upcoming fixtures.

When do we process personal data?

Virtually anything we do with personal data is processing including, collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure, or destruction. So even just storage of personal data is a form of processing. We may process personal data using computers or manually by keeping paper records.

Personal data

Personal data is data that relates to a living individual who can be identified from that data (or from that data and other information likely to come into our possession). The living individual may be an employee, customer or prospective customer, supplier, contractor or contact, and that personal data may be written, oral or visual (e.g.) CCTV.

Data will relate to an individual and therefore be their personal data if:

- It identifies the individual. For instance, names, addresses, telephone numbers and email addresses.
- Its content is about the individual personally. For instance, medical records, credit history, a recording of their actions or contact details.
- Relates to the property of the individual, for example their home, their car, or other possessions.
- It could be processed to learn, record, or decide something about the individual. For instance, if you can link the data to the individual to tell you something about them (e.g. salary details for a post where there is only one named individual in that post).

- Is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotation for them.
- Has the individual as its focus. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual.
- Affects the individual's privacy e.g. work email addresses can also be personal data.
- Is an expression of opinion about the individual or is an indication of our intentions towards the individual e.g. how a complaint about that individual will be dealt with.

Examples of personal data

- Unique names
- Names together with email addresses or other contact details
- Job title and employer if only one person in the position
- Video and photographic images
- Information about individuals because of safeguarding checks
- Medical and disability information
- CCTV images
- Member profile information (e.g. marketing preferences).
- Financial information and accounts.

Special category data

Some data falls into special categories where extra caution must be taken. These are highly sensitive categories of personal data, such as data about an individual's:

● racial or ethnic origin

● political opinions

● religious or philosophical beliefs

● genetic data

● biometric data for the purpose of uniquely identifying a natural person

● health; and

● sex life or sexual orientation.

Criminal records data has its own special category which is treated to some extent the same as other special category data.

There are enhanced rules in respect of such data, requiring additional justification for processing. Relevant justifications include receiving explicit consent from the individual; where the information has already been made public by the individual; or where it is a medical/health emergency.

Example: The County Buggy policy requires confirmation of a medical condition before allowing the use of buggies in certain competitions. In order to receive such information lawfully, the County will need to obtain the explicit consent from the individual to record their health information – meaning a documented consent, evidenced by a clear affirmative action (such as a signature confirmation), establishing freely given and specific agreement to the processing.

GDPR Principles

All personal data must be:

- Processed lawfully and transparently Personal data must always be processed fairly and lawfully and with transparency at the forefront of all processing. We must ensure that we have a solid and documented justification for how we use personal data (for example, keeping a record of consent from the individual that they are happy to receive information about County competitions).
- collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes (purpose limitation).
- must be adequate, relevant, and limited to what is necessary for the purpose for which we collect it (data minimisation). Example: If an Application Form requests details of an individual's ethnicity, unless you can demonstrate that this information is necessary, it would not comply with the 'data minimisation' principle to request this.
- must be accurate and, where necessary, kept up to date. Example: A player emails you to tell you that they are moving to a new address. You update the contact details you have and ensure that no further communications are posted to the old address.
- must be retained in a form that permits identification of individuals for no longer than is necessary. Example: You are holding competition contact records from several years ago that identify individuals who no longer enter competitions. Unless there was a good reason to keep these, December 2023 this would breach the requirement to keep personal data only for as long as necessary). Data security Personal data must be processed in a manner that ensures appropriate technical and organisational security of those data. This means staying abreast of developments in information security and ensuring that security measures (such as restricting access rights, patching known system flaws and providing staff training) are applied within your organisation.

Data subject rights

Those people that we hold data on have specific rights under the data protection laws. These are:

- The right to access their personal data, usually referred to as a subject access request.
- The right to have their personal data rectified.
- The right to have their personal data erased.
- The right to restrict processing of their personal data.
- The right to object to receiving direct marketing materials.
- The right to portability of their personal data.
- The right to object to processing of their personal data.
- The right to not be subject to a decision made solely by automated data processing.

The exercising of these rights may be made in writing and verbally and should be responded to by us within one month of receipt of the request. That period may be extended by two months where necessary. We must inform the individual of any such extension within one month of the request together with the reasons for the delay.

Where the data subject makes the request by electronic form, any information provided should also be in electronic form where possible, unless otherwise requested by the individual.

If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was in fact instigated by the individual and that the third party is properly authorised to make the request.

There are specific exemptions for some of these rights and not all of them are absolute rights. However, the right to not receive marketing is an absolute right and should be complied with immediately.

Where an individual considers that we have not complied with their request, they can seek a court order and compensation. If the court agrees with the individual, it will issue a court order to make us comply. The court can also award compensation.

Security Breaches

We ensure that any security breaches are notified to the ICO (Information Commissioner's Office) without undue delay and, where feasible, within 72 hours of awareness (unless the breach is "unlikely to result in a risk to the rights and freedoms" of data subjects – where we are unclear on this, a minimum of three members will make this decision and the decision will be documented as part of the breach (Data Protection Act December 2023).

ICO Contact Telephone Number 0303 123 1113.

Notification will also be made to the affected data subjects without undue delay.

Example: A mailing is inadvertently sent out to the entire County mailing list that contains a spreadsheet record of the health details of players that require Buggies. You are unable to successfully recall the email and you realise there were no password protections in place in the spreadsheet, therefore you consider that this situation may result in a high risk to the rights and freedoms of the individuals concerned.

You must inform the CGL without delay and the appropriate person will notify the Information Commissioner's Office and the affected individuals without undue delay. Under the GDPR, any data subject that has suffered damage because of an infringement of the GDPR will have a right to claim compensation for that damage from the infringing organisation.

Foreign transfer of personal data

The CGL does not transfer any data abroad.

Monitoring and review of our policy and the way we process data

We regularly check, analyse, review:

- Review what personal information we collect (for example players, employee, and volunteer information) – and the source of this information. Is it directly from the individual or from some another source, such as a club?

- How this data is used (which might be for competitions, marketing, employment, or administrative purposes) and cross-check those activities against the permitted conditions for processing, asking: why am I allowed to use this information?

- Check employment contracts, ensuring that adequate privacy information is provided to employees and volunteers.

- Check Internal data protection policies regularly and ensure any new Data Protection Legislation is included.

- Review who in our organisation has access to records containing personal data and determine whether it is necessary for everyone who currently has access to retain it

- Ensure that contracts that require personal data to be transferred to another organisation – which happens where you use a cloud-based software system, for example, are GDPR-compliant.

- the framework e.g. are the right people involved, both to take decisions and to undertake technical activities to try to minimise the scale of breach and consequences on data subjects.

- the practicalities e.g. how are they going to be contacted if a breach is discovered at 17.45 on a Friday or noon on a Sunday?

- We review internal processes for complying with individuals' rights. In particular, ensure December 2023 standard responses to subject access requests inform individuals about their other rights

record for the County and, on that basis, you retain the key information (e.g. entrant name, handicap, result) but remove information that is no longer necessary or relevant (e.g. contact details).

6: Data security Personal data must be processed in a manner that ensures appropriate technical and organisational security of those data. This means staying abreast of developments in information security and ensuring that security measures (such as restricting access rights, patching known system flaws and providing staff training) are applied within your organisation.

For standard personal information such as names, addresses, handicaps, contact details, the answer should be one of the following:

1. you have an individual's consent, evidenced by a clear affirmative action, establishing freely given and specific agreement to the processing Example: You need consent to sign up a member to receive promotional material from the County and for other products or services they might be interested in. You inform the individual about who their data will be passed to and how they might be contacted so that the individual can agree to the specifics. You then ask the member to tick a box to confirm their 'clear affirmative consent' to receive the mailings. (When you do rely on consent, the requirement for a clear affirmative act means the individual must take deliberate action to opt in).

2. the processing is necessary for performing a contract the individual is party to Example: Using someone's contact and payment details to complete a competition entry. Without their details, the transaction could not be completed and therefore you are justified in using their details for the purpose of making the sale/booking.

3. you are complying with a legal obligation Example: You are required to run DBS checks on volunteers who will undertake activities working with junior golfing groups. You need to provide information about the individuals to the England Golf Disclosure & Barring Service to do this.

4. the processing is necessary in order to protect the vital interests of the data subject or of another natural person Example: A volunteer working on the course collapses and emergency services are called. The volunteer's personal details will need to be provided to the emergency services in order for them to retrieve his medical information to protect the 'vital interests' (the key health situation) of that individual.

5. you are pursuing legitimate interests, except where those interests are overridden by the individual's rights Example: You email volunteers periodically to see if they are available to provide support on specific dates or at events. The Committee will have a legitimate interest in locating available volunteers and this outweighs the privacy rights of the volunteers, who will have an expectation that they will be contacted.

Privacy No5ces

The CGL have a privacy notice which can be found on the website.

Good Practice when dealing with personal data.

Whilst taking a common-sense approach, good practice guidelines should be adhered to**.**

- Do not disclose any unique logins or passwords.
- Never leave any items containing personal data unattended in a public place. This would include paper files, mobile phones, laptops, tablets, or memory sticks.
- Never leave any items containing personal data in unsecure locations e.g. in a car in your drive overnight. This would include paper files, mobile phones, laptops, tablets, or memory sticks.
- If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.
- Do lock laptops, files and removable storage devices containing personal data, away and out of sight when not in use.
- Do password protect documents and databases containing personal data.

- Never use removable storage media to store personal data unless the personal data on the media is encrypted.
- Use confidential waste disposal for any papers containing personal data or have them shredded prior to using ordinary waste disposal.
- Do dispose of any materials containing personal data securely, whether the data is paper based or electronic.
- When in a public place e.g. a train or a café, be careful as to who might be able to see the in information on the screen of any device you are using when you have personal information on display. If necessary, move location or change to a different task.
- Do ensure that you screen faces away from prying eyes if you are processing personal data, even if you are working in an office. Persona data should be accessed only by those who need to see it.
- Do not leave personal data lying around, store it securely.
- When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information. Instead use first names or initials to preserve confidentiality.
- Never act on instructions from someone unless you are sure of their identity and if you are unsure take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging e.g. involving money, health, criminal records.
- Do not transfer data to any third party without consent.
- Notify the club secretary immediately of any suspected security Breach or loss of data.

Any queries regarding this policy should be directed to the County Secretary
secretary@cheshiregolf.org.uk