LITTLE HAY GOLF CLUB

Data Protection Policy

Little Hay Golf Club is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our members, volunteers and consultants ("**Workers**").

This Data Protection Policy ("**Policy**") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

Little Hay Golf Club will comply with this Policy and apply and implement its requirements when processing any personal data. These include the practical day to day actions that Workers must adhere to when working or volunteering for the Club as set out below. All our Workers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

Any breaches of this Policy will be viewed very seriously and may result in disciplinary action, criminal sanctions, civil fines, court orders, claims for compensation, bad publicity or loss of business. All Workers must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedures.

1. Data Protection Laws

From 25th May 2018 a General Data Protection Regulation (**GDPR**) came into force, together with the Data Protection Act 2018 ("**DPA 2018**") ("**Data Protection Laws**"), after Brexit the UK will adopt laws equivalent to these Data Protection Laws.

This Policy states the position as from 25th May 2018.

The Data Protection Laws all require that the 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.

Key words in relation to data protection

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

Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. if a name or video footage) or might do if taken together with other information available to or obtainable to us (e.g. a job title and company name).

Data subject is the living individual to whom the relevant personal data relates.

Processing is widely defined under data protection law and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

Data processor is a person who processes personal data on behalf of LHGC and only processes that personal data in accordance with instructions from the LHGC.

2. Personal data held by LHGC.

- Names, addresses, telephone numbers and email addresses and contact details. These may include work email addresses.
- Photographic and Video images taken at Club events.
- Financial information such as that relating to Membership fees and Bank records.
- Juniors Parental and Medical information when joining.

Lawful basis for processing

For personal data to be processed lawfully, HGC will be processing it on one of the legal grounds set out in the Data Protection Laws.

Members will have given their consent to the processing of their data.

For the processing of ordinary personal data in our Club this may include, among other things:

The processing that is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions); or

The processing that is necessary for keeping in touch with members, players, participants about competition dates, upcoming fixtures or access to club facilities.

The processing that is necessary to record fees and charges relating to playing matches against other clubs.

Special category data

We do not save any Special Category personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data or genetic data.

.

Processing personal data

Processing that LHGC does includes collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of data. It is done using computers or manually by keeping paper records.

To support these processes, we. endeavour to :

Uphold the rights for individuals in respect of personal data that data controllers hold on them.

Process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly, lawfully and in a transparent manner).

Provide certain information to those individuals about whom we process personal data, this is provided in the privacy notice which each Worker will have received.

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); and

Keep adequate records of how data is processed and, where necessary, notify the'' Information Commissioner's Office' and possibly data subjects where there has been a data breach.

Ensure records are held securely and not longer than is necessary.

Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**"). The ICO has extensive powers.

The following describe the Data Protection principles and Data Subject rights which we strive to uphold.

3. Data protection principles

The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data will be:

1. Processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met.
2. Collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation").
3. Adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimization").
4. Accurate and where necessary kept up to date.
5. Kept for no longer than is necessary for the purpose (storage limitation").
6. Processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

4. Data subject rights

Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary 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, usually referred to as the right to be forgotten.
- 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; and
- The right to not be subject to a decision made solely by automated data processing.

5. Exercise of these Rights

The exercise of these Rights may be made in writing, including email, and also verbally and will be responded to in writing by LHGC without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months if necessary, considering the complexity and number of the requests. T h e individual will be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

If the request is in an electronic form, any information will be provided by electronic means where possible, unless otherwise requested by the individual.

If a request is received from a third party (e.g. a legal advisor), we will 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. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

If it is considered that we have not complied with the request e.g. exceeded the time period, a court order may be sought together with compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The ICO must investigate and may serve an “Information Notice” onus. The result of the investigation may lead to an “Enforcement Notice” being issued by the ICO.

6. What we will do:

Immediately notify the Club Welfare Officer (CWO) if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them.

Take care with all personal data and items containing personal data so that it stays secure and is only available to or accessed by authorised individuals; and

Immediately notify the CWO if there is a suspicion that there is the loss of any personal data or any item containing personal data. For more details on this, see our separate ‘Disciplinary

Regulations and Procedures' which applies to all our Workers regardless of their position or role in our organisation.

For suggestions as to how to use and safeguard personal data please see the attached document '**Practical matters in relation to Data Protection'.**

Practical matters in relation to Data Protection

Whilst you should always apply a common-sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

Do not take personal data out of the organisation's premises (unless absolutely necessary).

Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

Never leave any items containing personal data in unsecure locations, e.g.

In car on your drive over night and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

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 encrypt laptops, mobile devices and removable storage devices containing personal data.

Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

Do password protect documents and data bases containing personal data.

Never use removable storage media to store personal data unless the personal data on the media is encrypted.

When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.

Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc, and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

When in public place, e.g. a train or café, be careful as to who might be able to see the 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 your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.

Do challenge unexpected visitors or employees accessing personal data.

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, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

Never act on instructions from someone unless you are sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

..