General Data Protection Regulations (GDPR) Policy Document 2018

Definitions:

The Company	Hilton hall Community Association (HHCA).
Responsible Persons	Keith Jones Data Protection Officer. Debbie Cox Data Protection Officer.
Register of Systems	A register of all systems or contexts in which personal data is processed by the Company.
Reasons For & Use of Data	All data collected & maintained for the purpose of contacting members, clients, customers and parents (of children who attend sports and/or educational training sessions / classes), when dealing with individual's details that are required for public health and/or safeguarding issues and as emergency contact details.
Duration Data is to be Kept, Reviewed and/or Deleted	All data will be kept safely & securely and not be shared with any third parties or persons (except when required by law) and shall be reviewed annually. Data will be updated annually and will be deleted when the Company no longer has a contractual and/or legal right to hold data. Personal data (of members, clients, customers, parents of children, and children) will be deleted upon request (with the exception of data required by law for public health and/or safeguarding issues and/or making or defending a legal claim).
Rights of Persons, i.e. Members, Clients, Customers, Parents of Children (and Children & Vulnerable Adults)	We recognize and accept the rights of individuals, groups & companies regarding such data and the way they are regulated and applied: i.e. The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to automated decision-making including profiling.

Data protection principles:

The Company is committed to processing data in accordance with its responsibilities under the GDPR.
Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

General provisions:

- This policy applies to all personal data processed by the Company.
- The Responsible Person(s) shall take responsibility for the Company's ongoing compliance with this policy.
- This policy shall be reviewed annually.

General Data Protection Regulations (GDPR) Policy Document 2018

Lawful, fair and transparent processing:

- To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of Systems and this Register of Systems shall be reviewed annually.
- Individuals have the right to access their personal data and any such requests made to the company shall be dealt with in 14 days.

Lawful purposes:

- All data processed by the company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
- The Company shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's systems.

Data minimisation:

The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy:

- The Company shall take reasonable steps to ensure personal data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / Removal:

- To ensure that personal data is kept for no longer than necessary, the Company shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- The archiving policy shall consider what data should / must be retained, for how long, and why.

Security:

- The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

Breach:

If you have a concern about the way we are collecting and/or using your personal data, we ask that you raise your concern with us in the first instance, by contacting our Data Protection Officers (contact details above).
In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO

END OF POLICY

General Data Protection Regulations (GDPR) Policy Document 2018

Record of Processing Activities:

Data Protection Officer: Keith Jones; keithfdjones@aol.com
Data Protection Officer: Debbie Cox; debz1313@gmail.com

Purpose of Processing

- To obtain contact details of members so they can be informed about activities, events, closures, etc.
- Emergency contact information and next of kin incase of an emergency.
- Permissions for first aid, photographs, video to be used on social media.
- Consent of parents for participation, training, competitions, activities & events etc. with regards safe gaurding procedures and health & safety.
-

Categories for data subjects and the personal data collected

- Adult members 16 years of age (and over).
- Child members under 16 years of age (data completed by parents).
- Personal data; Surname, Forename, DOB, Home address, Telephone numbers, Two emergency contacts, consent for photos/video, etc.
- Sensitive personal data; Medical details, consent for first aid.
- Hirers of Hilton Hall Community Association (i.e. companies, community groups, social groups, sports groups hiring Hilton Hall Community Centre &/or Facilities).

Transfer of personal data

- Data may be shared with other members of the committee who need to contact members directly. Data will be shared securely using password encrypted files.
- Data will not be shared with any third parties or other members of the company not on the committee.

Information security

- Data will be stored in paper form in a securely lock cupboard accessible only by the Data Protection Officers (listed).
- Electronic data will be stored using password protected documents on an unnetworked computer.
- Company members, clients, customers and parents of children can ask for the data that we hold or for it to be deleted at any time (A few exceptions do occur such as when individual's details are required for public health/safeguarding issues and/or making or defending a legal claim). This will be done within 14 days.
- Any Backups of data will be stored on an external drive which will be kept in a securely locked cupboard.
- There is no obligation for the company to register the data we hold with the ICO.

Archiving and Erasure of information

The data that we hold as a Company will be reviewed annually.

For members who continue with the Company the following year data will be checked and updated to ensure all data is accurate (i.e contact details, emergency numbers and/or changes in medical conditions or personal details such as address, etc.). Unnecessary sensitive personal data will be deleted and personal data (such as names and contact details) will be stored for 5 years in order to keep members up to date with new information (after five years of non-activity all data will be deleted (including electronic data and/or any paper records which will be shredded and destroyed). New records will be stored as specified in the Record of Processing activities.

New members, clients, customers and parents of children (and those who have requested deletion of data) must apply and complete new membership forms / consent forms each year.