Cambridge University Aikido Club

Data Protection Policy

Cambridge University Aikido Club (the Club) is fully committed to complying with data protection law and to respecting the privacy rights of individuals.

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

The Policy applies to all of the Club's members and it is each member's responsibility to familiarise themselves with the Policy and to apply and implement its requirements when processing any personal data. Please pay special attention to sections 14, 15 and 16 as these set out the practical day-to-day actions to which members must adhere.

The Policy has been designed to ensure that members are aware of their legal requirements, and those of the Club, and to give practical guidance as to how to comply with them. The Policy also sets out the consequences of failing to comply with these legal requirements.

If at any time you have any queries on the Policy, your responsibilities or any aspect of data protection law, you should contact the Club Secretary.

1. Who is responsible for data protection?

1.1. All of the Club's members are responsible for data protection, and each one has a role to play to make sure that the Club is compliant with data protection laws.

1.2. We are not required by law to appoint a dedicated Data Protection Officer, but the Club's Secretary shall be responsible for overseeing our compliance with data protection laws.

2. Why do we have a Data Protection Policy?

2.1. We recognise that processing of individuals' personal data in a careful and respectful manner fosters trust. We believe that this will enable our Club to work more effectively with and to provide a better service to our members.

2.2. Any breaches of the Policy will be treated seriously. All members must read the Policy carefully and make sure they are familiar with it. Breaching the Policy is a disciplinary offence and will be dealt with under the Disciplinary Procedure set out in the Club's Constitution.

2.3. If a member of the Club or its Executive Committee has not complied with Data Protection Laws or the Policy, then they are encouraged to report this fact

immediately to the Secretary. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliance which may pre-date the Policy coming into force.

2.4. If a member of the Club or its Executive Committee believes that any other representative of the Club is not complying with Data Protection Laws or the Policy, they should report it in confidence to the Secretary.

3. Other consequences

3.1. There are a number of potentially serious consequences of non-compliance with Data Protection Laws for both individual members and for the Club. These may include:

a. For members:

i. Criminal sanctions: Serious breaches could potentially result in criminal liability.

b. For the Club:

i. Criminal sanctions: Non-compliance could involve a criminal offence.

ii. Civil Fines: These can be up to 20 million euros.

iii. Assessments, investigations and enforcement action: The Club could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

iv. Court orders: These may require the Club to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

v. Claims for compensation: Individuals may make claims for damage they have suffered as a result of non-compliance.

vi. Bad publicity: Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our reputation. Court proceedings are public knowledge.

vii. Loss of members: Prospective and existing members not want to be involved with the Club if we are seen to have been careless with personal data or to have disregarded our legal obligations.

viii. Use of time and resources: Dealing with assessments, investigations, enforcement action, complaints, claims, etc. takes time and effort and can involve considerable cost.

4. Data protection laws

4.1. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA 2018") (together "Data Protection Laws") apply to any personal data that the Club processes. After the UK leaves the European Union, it will adopt laws equivalent to these Data Protection Laws.

4.2. The Data Protection Laws require that personal data is processed in accordance with the Data Protection Principles (see below) and gives individuals rights to access, correct and control how the Club uses their personal data.

5. Key words in relation to data protection

5.1. 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 a member of the Club or its Committee, a prospective member, or a supplier of facilities or services, and that personal data might be written, oral or visual (e.g. video or photography).

5.2. 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 a photograph) or if taken together with other information available or obtainable (e.g. a job title and company name).

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

5.4. 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 collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including images.

5.5. Data controller is the person who decides how personal data is used. For example, the Secretary will always be a data controller in respect of personal data relating to our members.

5.6. Data processor is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example, the British Aikido Board's Secretary will be a data processor.

6. Personal data

6.1. Data will relate to an individual and be their personal data if it:

a. identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

b. is about the individual personally. For instance, their medical history or contact details;

c. relates to property of the individual, for example their home or other possessions;

d. could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual;

e. is biographical in a significant sense, in that it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them;

f. has the individual as its focus, in that the information relates to the individual personally rather than to some other person or a transaction or event he/she was involved in. For instance, if a committee meeting is called to discuss a member's conduct this would relate to the individual;

g. affects the individual's privacy, whether in their personal, family, organisation or professional capacity. For instance, email addresses can also be personal data;

h. is an expression of opinion about the individual; or

i. is an indication of the Club's (or any other person's) intentions towards the individual (e.g. if it indicates how a complaint made by that individual should be handled).

6.2. Examples of information likely to constitute personal data:

a. Unique names;

b. Names together with email addresses or other contact details;

c. Job title and employer (if there is only one person in the position);

d. Video or photographic images;

e. Information about individuals obtained as a result of Safeguarding checks;

f. Medical and disability information;

g. Member profile information (e.g. contact preferences); and

h. Financial information and accounts.

7. Lawful basis for processing

7.1. For personal data to be processed lawfully, we must be processing it for one of the reasons set out in the Data Protection Laws.

7.2. For the processing of ordinary personal data in our Club, these reasons may include, among other things:

a. the data subject has given their consent to the processing (when applying to be a member of the Club, for example);

b. the processing is necessary for the performance of a contract with the data subject (for example, for processing their membership fees);

c. the processing is necessary for compliance with a legal obligation to which the data controller is subject (such as reporting a serious training-related accident); or

d. the processing is necessary for the legitimate interest reasons of the data controller or a third party (for example, keeping in touch with members about upcoming Club events, seminars and competitions, or restrictions on access to training venues).

8. Special category data

8.1. Special category data under the Data Protection Laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sexual orientation or gender identity, biometric data and genetic data.

8.2. Under Data Protection Laws, this type of information is known as special category data. Criminal records history becomes its own special category which is sometimes treated the same as special category data.

8.3. To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

a. the processing is necessary to protect the vital interests of the data subject. The Information Commissioner's Office ("ICO") has previously indicated that this condition is unlikely to be met other than in a life-or-death, or similarly extreme, situation;

b. the processing relates to information manifestly made public by the data subject;

c. the processing is necessary for the purpose of establishing, exercising or defending legal claims; or

d. the processing is necessary for the purpose of preventative medicine.

8.4. To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

a. ensure that either the individual has given their explicit consent to the processing; or

b. ensure that our processing of that criminal records history is unavoidable due to a legal requirement imposed upon us.

8.5. We would normally only expect to process special category personal data or criminal records history data usually in the context of our members or coaches for health and safety requirements, safeguarding checks, etc.

9. When do we process personal data?

9.1. Virtually anything the Club does with personal data is considered processing, including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. Even storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

9.2. Examples of processing personal data might include:

a. Using personal data to correspond with members; and

b. Holding personal data in our databases or documents.

10. Outline

10.1. The main themes of the Data Protection Laws are:

a. good practices for handling personal data;

b. rights for individuals in respect of personal data that data controllers hold on them; and

c. being able to demonstrate compliance with these laws.

10.2. In summary, data protection law requires each data controller to:

a. only process personal data for certain purposes;

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

c. provide certain information to those individuals about whom we process personal data, which is usually provided in a privacy notice;

d. 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

e. keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a data breach.

10.3. Every member of the Club has an important role to play in achieving these aims. It is the responsibility of each member to familiarise themselves with the Policy.

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

11. Data protection principles

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

a. processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

b. collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

c. adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

d. accurate and where necessary kept up to date;

e. kept for no longer than is necessary for the purpose ("storage limitation");

f. processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

12. Data subject rights

12.1. Under Data Protection Laws individuals have certain rights (Rights) in relation to their own personal data. In summary these are:

a. The rights to access their personal data, usually referred to as a subject access request

b. The right to have their personal data rectified;

c. The right to have their personal data erased, usually referred to as the right to be forgotten;

d. The right to restrict processing of their personal data;

e. The right to object to receiving direct marketing materials;

f. The right to portability of their personal data;

g. The right to object to processing of their personal data; and

h. The right to not be subject to a decision made solely by automated data processing.

12.2. The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by the Club (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

12.3. Where the data subject makes the request by electronic means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

12.4. 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. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

12.5. There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However, the right to not receive marketing material is an absolute right, so this should be complied with immediately.

12.6. Where an individual considers that the Club has not complied with their request e.g. exceeded the time period, 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. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

12.7. 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 on the Club (if we are the relevant data controller). The result of the investigation may lead to an Enforcement Notice being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to the Secretary from the ICO.

12.8. In the event of a Club member receiving such a notice, they must immediately forward the communication to the Club's Secretary.

13. Notification and response procedure

13.1. If a member has a request for the exercise of a Right, they should inform the Club's Secretary of the request.

13.2. If a letter or email exercising a Right is received by any member, they should log the receipt of the letter with the Secretary and send a copy of it to them. The Secretary will then respond to the data subject on our behalf.

13.3. The Secretary will co-ordinate our response [which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request. The Secretary will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the Secretary should suffice in most cases.

13.4. The Secretary will inform the Executive Committee of any action that must be taken to legally comply.

13.5. The Secretary's reply will be validated by the Executive Committee. For more complex cases, the Executive Committee may seek guidance from external legal advisors.

14. Obligations of ordinary members

14.1. What this all means for you as a member of the Club can be summarised as follows:

a. Treat all personal data with respect;

b. Treat all personal data how you would want your own personal data to be treated;

c. Notify the Club's Secretary at the earliest opportunity if any individual gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

d. Take care with all personal data (and items containing personal data) that you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

e. Immediately notify the Secretary if you become aware of or suspect the loss of any personal data or any item containing personal data.

15. Obligations of the Executive Committee

15.1. Data protection laws have different implications for different aspects of the Club's activities. Activities particularly affected by data protection law include Membership, Events and Promotions, Safety, Welfare and Finance.

15.2. As a member of the Executive Committee, you must consider what personal data you might handle, consider carefully what data protection law might mean for you and your responsibilities to the Club, and ensure that you comply at all times with the Policy.

16. Practical matters

16.1. 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:

a. Use passwords to protect documents and databases containing personal data.

b. Never disclose unique logins or passwords for any of the Club's accounts and databases to anyone other than authorised individuals.

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

d. Never leave any items containing personal data unattended in a public place or in an unsecure location. This applies to paper files, mobile phone, laptops, USB memory sticks, etc.

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

f. Store personal data securely and use encryption to secure laptops, mobile devices and removable storage devices containing personal data. Lock those devices away and keep them out of sight when not in use.

g. When in a public place, such as 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 data on display. Personal data should only be accessed and seen by those who need to see it.

h. 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 only first names to maintain confidentiality.

i. Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity.

j. Do not transfer personal data to any third party without prior written consent of the Club's Secretary.

k. Notify the Secretary immediately of any suspected security breaches or loss of personal data.

l. If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the Secretary.

17. Foreign transfers of personal data

17.1. Personal data must not be transferred outside the European Economic Area (EEA) unless the destination country ensures an adequate level of protection for the rights of

the data subject in relation to the processing of personal data or we put in place adequate protections. This is mainly relevant to data held and accessed in Cloud-based services as well as any data processing the Club may decide to outsource.

17.2. Members must not under any circumstances transfer any personal data outside of the EEA without the approval of the Secretary, who should themselves seek the approval of the Executive Committee.

17.3. The Club will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data outside of the EEA.

17.4. If you are involved in any new processing of personal data which may involve transfer of personal data outside of the EEA, then please seek the approval of the Secretary prior to implementing any processing of personal data that may have this effect.

18. Queries

18.1. If you have any queries about the Policy, please contact the Club's Secretary.