



KAIZEN MARTIAL ARTS ACADEMY

DATA PROTECTION POLICY

Our Policy

Kaizen Martial Arts Academy is committed to complying with data protection law and respecting individuals' privacy rights. The policy applies to all Kaizen members.

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

We recognise that you have an essential role in achieving these aims. Therefore, It is your responsibility to familiarise yourself with this Policy and 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 you must adhere to when teaching, training or volunteering for the Academy.***

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also outlines the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor our or your responsibilities concerning data protection.

If you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice.

Who is responsible for data protection?

1.1 All our Instructors are responsible for data protection, and each person has a role to play in ensuring that we comply with data protection laws.

1.2 We are not required to appoint a Data Protection Officer (DPO), but we have chosen to do so. Jim Reece will 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 individuals' personal data carefully and respectfully cultivates trusting relationships with those individuals and trust in our brand. We believe such relationships will enable our organisation to work more effectively with and provide better service to those individuals.

2.2 This Policy works with other policies we implement from time to time and any other policies we implement from time to time.

3. Status of this Policy and the implications of breach.

3.1 Any breaches of this Policy will be viewed very seriously. All Instructors must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be handled under our Disciplinary Procedure.

3.2 If you do not comply with Data Protection Laws and/or this Policy, you are encouraged to report this fact immediately to Jim Reece. This self-reporting will be considered in assessing how to deal with any breach, including any non-compliance that may predate this policy coming into force.

3.3 Also, if you are aware of or believe that any other representative of ours is not complying with Data Protection Laws and/or this Policy, you should report it to Jim Reece in confidence.

4. **Other consequences**

4.1 There are several severe consequences for you and us if we do not comply with Data Protection Laws. These include:

4.1.1 For you:

4.1.1.1 **Disciplinary action:** Failure to comply with our policies could lead to termination of your position with us if you are an instructor or volunteer.

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

4.1.1.3 **Investigations and interviews:** Your actions could be investigated, and you could be interviewed concerning any non-compliance.

4.1.2 For Kaizen Martial Arts Academy:

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

4.1.2.2 **Civil Fines:** These can be up to Euro 20 million or 4% of the group's worldwide turnover, whichever is higher.

4.1.2.3 **Assessments, investigations and enforcement action:** We 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.

4.1.2.4 **Court orders:** These may require us to implement measures or take steps concerning or cease or refrain from processing personal data.

4.1.2.5 **Claims for compensation:** Individuals may make claims for damage they have suffered because of our non-compliance.

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

4.1.2.7 **Loss of business:** Prospective members, participants, players, customers, suppliers and contractors might not want to deal with us if we are viewed as careless with personal data and disregarding our legal obligations.

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

5. **Data protection laws**

5.1 The General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") (together with "**Data Protection Laws**"), and then after Brexit, the UK will adopt laws equivalent to these Data Protection Laws.

5.2 The Data Protection Laws all require that the personal data is processed in accordance with the Data Protection Principles (see below) and give individuals rights to access, correct and control how we use their personal data (see below).

6. **Keywords in relation to data protection**

- 6.1 **Personal data** 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, a customer, a prospective customer, a supplier, a contractor or a contact, and personal data might be written, oral or visual (e.g. CCTV).
- 6.2 **Identifiable** means that the individual can be distinguished from a group of individuals (although that individual's name need not be ascertainable). The data might identify an individual on its own (e.g. a name or video footage) or might do so if taken together with other information available to or obtainable to us (e.g. a job title and company name).
- 6.3 **Data subject** is the living individual to whom the relevant personal data relates.
- 6.4 **Processing** is widely defined under data protection law. 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.
- 6.5 **A data controller** is the person who decides how personal data is used; for example, we will always be a data controller concerning personal data relating to our members
- 6.6 **A data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data under instructions from the data controller.

7. **Personal data**

- 7.1 Data will relate to an individual and therefore be their data if it:
- 7.1.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
 - 7.1.2 its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;
 - 7.1.3 relates to the property of the individual, for example, their home, their car or other possessions;
 - 7.1.4 it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you can link the data to the individual to tell you something about them, this will relate to the individual;
 - 7.1.5 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 connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation meeting, this may not relate to the individual and may be more likely to relate to the company they represent;
 - 7.1.6 has the individual as its focus; that is, the information relates to the individual personally rather than to some other person or a transaction or event he was involved in. For instance, if a meeting is to discuss the individual's performance, this is likely to relate to the individual;
 - 7.1.7 affects the individual's privacy, whether in their personal, family, organisation or professional capacity; for instance, email address or location and work email addresses can also be personal data;
 - 7.1.8 is an expression of opinion about the individual or

7.1.9 indicates our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

7.2 Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers, employees, and sole traders or partners is often personal data, so business-related information can often be personal data.

7.3 Examples of information likely to constitute personal data:

7.3.1 Unique names;

7.3.2 Names together with email addresses or other contact details;

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

7.3.4 Video and photographic images;

7.3.5 Information about individuals obtained because of Safeguarding checks;

7.3.6 Medical and disability information;

7.3.7 CCTV images;

7.3.8 Member profile information (e.g. marketing preferences) and

7.3.9 Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

8. **Lawful basis for processing**

8.1 For personal data to be processed lawfully, we must process it on one of the legal grounds set out in the Data Protection Laws.

8.2 For the processing of ordinary personal data in our organisation, these may include, among other things:

8.2.1 the data subject had given their consent to the processing (perhaps on their membership application form or when they registered on the club's website)

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

8.2.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject (such as reporting payments to instructors to the tax authorities) or

8.2.4 the processing is necessary for the legitimate interest of the data controller or a third party (for example, keeping in touch with members, players, and participants about competition dates, upcoming fixtures or access to club facilities).

9. **Special category data**

9.1 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, sex life, biometric data and genetic data.

9.2 Under Data Protection Laws, this type of information is known as special category data and criminal records history becomes its own special category, which is treated for some parts the same as special category data. Previously, these types of personal data were referred to as sensitive personal data, and some people may continue to use this term.

- 9.3 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:
- 9.3.1 the processing is necessary for the performance of our obligations under employment law;
 - 9.3.2 processing is necessary to protect the data subject's vital interests. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;
 - 9.3.3 the processing relates to information manifestly made public by the data subject;
 - 9.3.4 the processing is necessary for establishing, exercising or defending legal claims or
 - 9.3.5 the processing is necessary for preventative or occupational medicine or the assessment of the employee's working capacity.
- 9.4 To lawfully process personal data relating to criminal records and history, there are even more limited reasons, and we must either:
- 9.4.1 ensure that either the individual has given their explicit consent to the processing or
 - 9.4.2 Ensure that our processing of those criminal records' history is necessary under a legal requirement imposed upon us.
- 9.5 We would typically only expect to process special category personal data or criminal records history data, usually in a personnel context and the context of our members/athletes/coaches/volunteers, for monitoring performance, drug and alcohol testing, health and safety requirements, safeguarding checks, etc.
- 9.6 **When do we process personal data?**
- 9.7 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 might process personal data using computers or manually by keeping paper records.
- 9.8 Examples of processing personal data might include:
- 9.8.1 Using personal data to correspond with members;
 - 9.8.2 Holding personal data in our databases or documents and
 - 9.8.3 Recording personal data in personnel or member files.
10. **Outline**
- 10.1 The main themes of the Data Protection Laws are:
- 10.1.1 good practices for handling personal data;
 - 10.1.2 rights for individuals in respect of personal data that data controllers hold on them; and
 - 10.1.3 being able to demonstrate compliance with these laws.
- 10.2 In summary, data protection law requires each data controller to:
- 10.2.1 only processes personal data for specific purposes;

- 10.2.2 process personal data following the six principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);
 - 10.2.3 provide certain information to those individuals about whom we process personal data, which is usually provided in a privacy notice; for example, you will have received one of these from us as one of our Workers;
 - 10.2.4 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
 - 10.2.5 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 Instructor/Volunteer has a vital role in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.
- 10.4 The Information Commissioner's Office ("ICO") enforces data protection laws in the UK. The ICO has extensive powers.
- 11. Data protection principles**
- 11.1 The Data Protection Laws set out six principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:
- 11.1.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
 - 11.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");
 - 11.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");
 - 11.1.4 accurate and, where necessary, kept up to date;
 - 11.1.5 kept for no longer than is necessary for the purpose ("storage limitation");
 - 11.1.6 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) concerning their personal data. In summary, these are:
- 12.1.1 The rights to access their data, usually referred to as a subject access request
 - 12.1.2 The right to have their data rectified;
 - 12.1.3 The right to have their data erased, usually referred to as the right to be forgotten;
 - 12.1.4 The right to restrict processing of their data;
 - 12.1.5 The right to object to receiving direct marketing materials;
 - 12.1.6 The right to portability of their data;
 - 12.1.7 The right to object to the processing of their data; and
 - 12.1.8 The right not to 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 verbally and should be responded to in writing by us (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, considering the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request and the reasons for the delay.
- 12.3 Where the data subject requests by electronic form 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 verify that the individual instigated the request and that the third party is properly authorised to make the request. This usually means contacting the relevant individual directly to confirm that the third party is properly authorised to make the request.
- 12.5 There are very specific or partial exemptions for some of these Rights, and not all 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 we have not complied with their request e.g. exceeded the 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 us (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 Jim Reece from the ICO.
- 12.8 If an Instructor/Volunteer receives such a notice, they must immediately pass the communication to Jim Reece.

13. **Notification and response procedure**

- 13.1 If a member has a request or believes they have a request for the exercise of a Right, they should:
 - 13.1.1 pass the call to their Instructor. The Instructor should take and record all relevant details and explain the procedure. If possible, get the request confirmed in writing and addressed to Jim Reece.
- 13.2 If any member receives a letter or fax exercising a Right they should:
 - 13.2.1 pass the letter to their Instructor;
 - 13.2.2 the Instructor must log the receipt of the letter with Jim Reece and send a copy of it to them and
 - 13.2.3 Jim Reece will then respond to the data subject on our behalf.
- 13.3 If an email exercising a Rights is received by any member, they should:
 - 13.3.1 pass the email to their Instructor;
 - 13.3.2 The supervisor/manager must log the receipt of the email with Jim Reece and send a copy of it to them and
 - 13.3.3 Jim Reece will then respond to the data subject on our behalf.

13.4 Jim Reece will coordinate our response, which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request. Jim Reece will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email should suffice in most cases.

13.5 Jim Reece will inform the relevant Instructor of any action that must be taken to comply legally.

13.6 The instructor who receives the request will ensure that the relevant response is made within the required period.

14. **Your main obligations**

14.1 What this all means for you can be summarised as follows:

14.1.1 Treat all personal data with respect;

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

14.1.3 Immediately notify your Instructor or Jim Reece if any individual says or does anything which gives the appearance of them wanting to invoke any rights concerning personal data relating to them;

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

14.1.5 Immediately notify Jim Reece if you become aware of or suspect the loss of any personal data or any item containing personal data. For more details on this see our separate Data Breach Policy which applies to all our Workers regardless of their position or role in our organisation.

15. **Your activities**

15.1 Data protection laws have different implications in different areas of our organisation and for different types of activity, and sometimes these effects can be unexpected.

15.2 Areas and activities particularly affected by data protection law include personnel matters, security (e.g. CCTV), customer care, sales, marketing and promotions, health and safety and finance.

15.3 You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply always with this 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:

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

16.1.2 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.

16.1.3 Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

16.1.4 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.

- 16.1.5 Do encrypt laptops, mobile devices and removable storage devices containing personal data.
- 16.1.6 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.
- 16.1.7 Do password protect documents and databases containing personal data.
- 16.1.8 Never use removable storage media to store personal data unless the personal data on the media is encrypted.
- 16.1.9 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.
- 16.1.10 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.
- 16.1.11 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
- 16.1.12 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.
- 16.1.13 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.
- 16.1.14 Do challenge unexpected visitors or employees accessing personal data.
- 16.1.15 Do not leave personal data lying around, store it securely.
- 16.1.16 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.
- 16.1.17 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.
- 16.1.18 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.
- 16.1.19 Do not transfer personal data to any third party without prior written consent of Jim Reece.
- 16.1.20 Do notify your Instructor or Jim Reece immediately of any suspected security breaches or loss of personal data.
- 16.1.21 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to Jim Reece

16.2 However, you should always take a common-sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of Jim Reece.

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 some data processing the club may outsource.

17.2 These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or because the recipient's own country's laws provide sufficient protection.

17.3 These restrictions also apply to transfers of personal data outside of the EEA even if the personal data is not being transferred outside of our group of companies.

17.4 You must not under any circumstances transfer any personal data outside of the EEA without Jim Reece's prior written consent.

17.5 We 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.

17.6 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 approval of Jim Reece prior to implementing any processing of personal data which may have this effect.

18. **Practical Application Specific to Kaizen Martial Arts Academy**

18.1 Anyone joining Kaizen must be asked to complete, or be assisted to complete, an enrolment form specific to that martial art. They should be given privacy to complete that form so that where possible the information cannot be seen by anyone.

The form should only be handed back to the instructor in charge who will make a note of the student's name in the register and place the form in a labelled folder in the office. The office should only be accessed by the instructor in charge and locked at the end of the evening.

Should the student/parent/guardian indicate on the form any medical or disability issues that need specific attention this should be discussed with sensitivity with the student/parent/guardian. It may be necessary to share this with key instructors but only with explicit consent for the purposes of providing the appropriate support during training.

18.2 The student/parent/guardian will already have been issued with a licence application form, photo consent forms and standing order form which, they will bring duly completed. If Jim Reece is not in attendance due to holidays or meetings the same care must be taken with the forms and placed in the labelled folder in the office.

18.3 The student's data is transferred to an encrypted database held by Jim Reece and the forms destroyed.

18.4 It is however necessary to keep a register of emergency contacts for each person. This is kept in the attendance binder which is locked away following the sessions.

When the student has left Kaizen, all records which could identify him/her are destroyed after six months except where specific aspects may be retained for statistical or legal purposes. This Consent must still be obtained.

19. **Queries**

19.1 If you have any queries about this Policy, please contact either your instructor or Jim Reece.

20. **Policy Review**

20.1 This policy will be subject to review in January 2025.