Stealth Martial Arts Privacy Notice

Our contact details

Name: Jason Burton

Phone Number: 07716 308030

E-mail: Jason@stealthmartialarts.com

ICO registration: ZB336297

Dates Policy amended: 1/7/24, 23/6/25

Date of Policy review: 23/6/25

Our Commitment to your Privacy

We respect your privacy and are committed to ensuring we do all we can to minimise the amount of data we hold about you and to treat it with respect and in line with the Data Protection Act 1988.

What type of information we have

We currently collect the following information:

• Personal information including Names, Contact details and relevant medical details, photos of students whose parents/guardian have consented to us taking.

How we get the information and why we have it

The personal information we hold is provided to us directly by you for one of the following reasons:

- To contact you with relevant information regarding our classes and payments including attendance register
- To ensure the health and safety of all members and that you are fit to train and are aware of the health implications of training
- To ensure our terms and conditions are understood and to keep a record of this

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

(a) Your consent. You are able to remove your consent at any time. You can do this by contacting **jason@stealthmartialarts.com**

(c) We have a legal obligation

(d) We have a vital interest to maintain health and safety

(e) We need it to perform a public task under government Test and Trace guidelines

(f) We have a legitimate interest.

What we do with the information we have

We use the information that you have given us in order to maintain good practice for health and safety and club updates.

We will only ever share information to fulfil any legal or safeguarding obligation with authorities or our governing body.

Photos and Images of students and staff are taken and used for promotional purposes on our social media but only where permission has been granted by the student themselves and the student's parent or legal guardian if a child or vulnerable adult.

Data Minimisation

We ask our staff members/volunteers and members for the following information and is the minimum amount required for the lawful purpose.

Name, address, date of birth, phone number and email address – for contact details to inform you of important updates to your sessions, for safeguarding purposes, in rare instances we need student details to share with authorities in case of a serious safeguarding issue or medical emergency. This information is also required to activate your personal insurance through us.

Emergency contacts – This is a requirement for our use in an emergency

Medical and health information – This information ensures we fulfil our commitment to your health and safety while with us, to tailor our sessions to ensure inclusivity and to share with relevant professionals should you experience a medical emergency and are unable to convey this information yourself.

From time to time we may ask for data about your ethnicity, gender and locality and other relevant information for any specific research in to our members which will be anonymous. This is taken to ensure we monitor and adapt how we deliver our sessions and our marketing to ensure we are consistently improving accessibility to our club across the whole community. Although anonymous, we still treat this information within ICO guidelines.

In addition to the above Staff and volunteers are required to complete an enhanced DBS check and all mandatory training as a minimum. These are held on file to fulfil our legal obligations and are only accessible by the lead instructor, Jason Burton.

How we store your information

Your information is securely stored in a locked filing cabinet for paper copies and held with us in a folder at sessions for health and safety purposes and emergency situations.

Digital copies are stored on password and virus protected devices that are only accessed by the Lead Instructor and the Course/Administration Assistant. No other staff members or volunteers can access this information.

We keep club membership Terms and Conditions and injury waiver forms for 1 year after leaving the club unless any specific . We will then dispose your information by shredding relevant documentation.

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal data in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at jason@stealthmartialarts.com if you wish to make a request.

Data Breaches – Our Process

Any breaches, suspected breaches or near misses of a breach will be taken extremely seriously and immediate action will be taken.

We will first risk asses the breach, suspected breach or near miss. If it is found that the privacy of personal or identifiable data has been breached we will notify those persons involved immediately with a full explanation of what data has been compromised, how, when and where.

We will then inform the ICO within 72 hours of us being informed or made aware of the breach, who will then further investigate and take action as deemed necessary. This will range from advice and logging to legal proceedings depending on the severity and the cause.

All incidents are logged to help us identify areas we may need to assess to ensure we fulfil our commitments to protecting personal data and personal privacy of all staff, volunteers and members/students.

As with any security incident, we will investigate whether or not the breach was a result of human error or a systemic issue. This will help us to ensure a recurrence can be prevented. To prevent breaches happening we have the following processes in place and communicated to all staff and volunteers. In the occurrence of a data breach the following will be re-visited earlier than the annual data protection training we provide in house.

- mandatory data protection induction and refresher training;
- support and supervising until our staff are proficient in their role.
- updating policies and procedures so all should feel able to report incidents of near misses;
- working to a principle of “check twice, send once”;
- implementing a culture of trust – everyone should feel able to report incidents of near misses;
- investigating the root causes of breaches and near misses; and
- protecting our employees and the personal data they are responsible for, including:
- Restricting access and auditing systems, or
- Implementing technical and organisational measures, eg disabling autofill.

Data Auditing and Monitoring

The Lead Data Protection Officer, Jason Burton, takes weekly audits of what information we have on file, who can access and how it has been used to ensure we consistently only store the minimum amount of data required and to remove data when requested, that back up files have not been taken and that our security software is running as it should. We date check data to ensure it is removed in a timely fashion and in line with our legal obligations for specific data we hold on file.

Data is also audited and anonymised to track any health and safety matters, accidents, incidents and concerns to ensure our staff training and all our procedures are effective and consistently improving. Key factors in our monitoring and audit processes:

1. **Review Existing Policies and Procedures**: We review our current policies and consent forms to ensure they align with legal requirements and our governing bodies regulations at a minimum of once a year but our target is once a month.
2. **Inventory of Data Storage and processing**: We have an inventory of all data types that we hold, why and where and we constantly check this is secure and that passwords are changed frequently.
3. **Assess Compliance with Data Protection Act 1988**: We evaluate whether our data handling practices adhere to privacy principles such as transparency, permissions, data minimisation and deletion timescales.
4. **Identify Risks**: We asses monthly to identify potential vulnerabilities in our data protection practices. Address any gaps or weaknesses. Ensure staff and volunteers are aware of their obligations and offer support and training where needed.
5. **Evaluate Third-Party Policies**: We assess the compliance with data protection regulations of all organisations we engage with. We ensure they follow the same standards as our organisation and hold ICO registration and have a Privacy policy.
6. **Document Findings and Recommendations**: We regularly document our audit findings, including areas of improvement and recommended actions enabling us to effectively review and update our policies based on these findings.

How to complain

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113