

Data Protection Policy

1. Introduction

The UKBJJA needs to collect and use certain types of information about the individuals and associations who are affiliated to the Association in order to carry on its work. This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998 and requirements of the [General Data Protection Regulation \(GDPR\)](#).

2. Disclosure

The UKBJJA may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The UKBJJA will not share data with third parties for commercial gain.

The Individual/Organisation will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the UKBJJA to disclose data (including sensitive data) without the data subject's consent.

These are:

- a) Carrying out a legal duty or as authorised by the Secretary of State
- b) Protecting vital interests of an Individual/Organisation or other person
- c) The Individual/Organisation has already made the information public
- d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- e) Monitoring for equal opportunities purposes – i.e. race, disability or religion
- f) Providing a confidential service where the Individual/Organisation's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Organisation to provide consent signatures.

The UKBJJA regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

The UKBJJA intends to ensure that personal information is treated lawfully and correctly.

To this end, the UKBJJA will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998 and requirements of GDPR.

Specifically, the Principles require that personal information:

- a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
- b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
- c) Shall be adequate, relevant and not excessive in relation to those purpose(s)
- d) Shall be accurate and, where necessary, kept up to date,
- e) Shall not be kept for longer than is necessary,
- f) Shall be processed in accordance with the rights of data subjects under the Act,
- g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Organisations in relation to the processing of personal information.

The UKBJJA will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
 - The right to be informed that processing is being undertaken,
 - The right of access to one's personal information
 - The right to prevent processing in certain circumstances and

- The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data collection

Informed consent is when:

- An Individual/Organisation clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

The UKBJJA will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, the UKBJJA will ensure that the Individual/Organisation:

- a) Clearly understands why the information is needed
- b) Understands what it will be used for and what the consequences are should the Individual/Organisation decide not to give consent to processing
- c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- e) Has received sufficient information on why their data is needed and how it will be used

5. Data Storage

Information and records relating to individuals and organisations will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is the Data Controller's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6. Data access and accuracy

All Individuals/Organisations have the right to access the information the UKBJJA holds about them. The UKBJJA will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, the UKBJJA will ensure that:

- It has a Data Protection Officer with responsibility for ensuring compliance with Data Protection
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and requirements of GDPR.

In case of any queries or questions in relation to this policy please contact the UKBJJA's designated Data Protection Officer.

7. Database of Members

1. The central records of the UKBJJA are kept on a computer database, maintained by the appointed officer.

2. Only officers stipulated by the Board, who have need to access information within the database in order to carry out their duties, may have access to some or all of the information on the database.

3. Any officer who is given access to information in the database must have received appropriate training and, where appropriate, a DBS check.

4. Information which may be entered into the database will be from

(a) personal membership application forms, signed by the applicant (or by the parent/legal guardian if the applicant is under the age of 18 years)

(b) club membership application forms, signed by the applicant

5. Membership forms will include a statement:

It is a requirement of the Data Protection Act 1998 that persons give their written authorisation to have their details recorded. By signing this application form, you are giving permission for your personal details to be recorded in the databases of the UKBJJA. These databases are not distributed to any other third party and are not used for non-BJJ related functions. Failure to sign the application will mean you cannot be a member of the UKBJJA.

Individual membership forms will carry a similar statement, with the final sentence: For persons under the age of 18 please ensure a parent or legal guardian signs on your behalf.

6. Annual membership renewals – if required a renewal form is completed any amendments are transferred into the database.

7. The records of an individual or club will be transferred by the appropriate officer into an 'archive' section of the database if, after 1 year, no renewal of membership has been received.

8. The records of an individual or club will be deleted by the Registrar from the database 5 years after archiving if no renewal has been received.
9. Paper records of membership applications will be destroyed after a total of 5 years.
10. No data on individuals generated from the database will be automatically published on the internet.
11. Where information is to be published on the internet, data will only be collected on forms specifically warning persons that the data may be posted on the web.
12. In the case of the UKBJJA wishing to post other information on individuals e.g. courses, officials, photographs of individuals, a separate form will be used.
13. Computer systems containing personal information on behalf of the Association must be secure and password protected.
14. The database must be password protected.
15. Other authorised officials will be supplied with minimal information as necessary to enable them to complete their tasks e.g. Treasurer will be sent financial and club contact information, competition organiser the status of membership of a participating competitor at an authorised event.
- 16 All paper records containing personal information must be secured in a locked cupboard or cabinet.
17. All personal information held in paper form is destroyed by shredding. CDs are broken.
18. Access to personal information. Under the Data Protection Act, individuals are entitled to see the records relating to them. Such a request should be submitted in writing to the UKBJJA's CEO or Data Protection Officer. The Association will supply the information within 30 working days of receipt of the request.