The British Kendo Association



Data Protection Policy

Last updated	02/05/2025

Definitions

Organisation	**The British Kendo Association**
DPA	Applicable Act - Data Protection Act 2018 which implements the EU's General Data Protection Regulation.
Responsible Person	Gerry Kincaid, Data Protection Officer (DPO)
Register of Systems	Refers to a register of all systems or contexts in which personal data is processed by the Association e.g. membership records, complaints, documentation systems, coaching records and mailing lists. This includes all associated technologies includes Servers, Databases, Mailers and Websites

1. Data protection principles

The Association is committed to processing data in accordance with its responsibilities under the DPA.

Compliance

DPA requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals records.
b. 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;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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 DPA in order to safeguard the rights and freedoms of individuals; and
f. 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.

2. General provisions

a. This policy applies to all personal data processed by the Association.
b. The Responsible Person shall take responsibility for the Association's ongoing compliance with this policy including annual reviews as required.
c. The Role of Data Protection Officer – DPO shall be a formal Office within the Association
d. This policy shall be reviewed annually.
e. A systems review will take place on an annual basis

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Association shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed annually.
c. Individuals have the right to access their personal data and any such requests made to the Association shall be dealt with in a timely manner subject to authentication via proof of ID, either a copy of a passport or driving licence; and proof of address, either a copy of a bank statement, utility bill, or TV licence. Identity theft is a reality and access to personal data must be authenticated as should any formal requests e.g. SAR
d. Where access is appropriate a fee may be applicable depended on the amount of work involved in it's provision.

4. Lawful purposes

a. All data processed by the Association must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The Association shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. 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 Association's systems e.g. The Association member mailing lists.

5. Data minimisation

a. The Association shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. Member records including grading records will be maintain in accordance with this and only necessary data will be maintained.

6. Accuracy

a. The Association shall take reasonable steps to ensure personal data is accurate. It is also the responsibility of each member to inform the Association of any changes to information held – address, contact information etc.
b. The Association holds the minimum amount of personal date relevant to maintaining membership records.
c. No data is held for marketing purposes and no data is shared external to the Association other that EKF records – grading, panel accreditation etc.
d. 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.
e. Only grading records will be updated on external systems – EKF register of member and members grades and panel and Shimpan accreditation

7. Archiving / removal

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

8. Security

a. The Association shall ensure that personal data is stored securely.
b. 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. This should be via named system Administrators.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

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. This includes cyber attacks. In the event thereof the Association shall promptly assess the risk to people's rights and freedoms.

END OF POLICY