THE KENDO ASSOCIATION OF HONG KONG, CHINA

GUIDELINES AND PROCEDURES ON PERSONAL DATA PRIVACY PROTECTION

Objective: *To demonstrate the Kendo Association of Hong Kong, China Limited's ("HKKA") commitment to respecting personal data privacy and complying with the data protection principles and all relevant provisions of the Personal Data (Privacy) Ordinance (Cap. 486), consistent with article 70A of Part B of the Articles of Association.*

This document applies to all Executive Committee Members, Senate Members, members of any committee or sub-committee of the Executive Committee, and to staff, coaches, referees, athletes and members of the HKKA, irrespective of the terms on which they are engaged (including short-term, part-time or voluntary capacities), and to every other person taking part in HKKA's business, activities, competitions, matches or events.

1. Privacy Policy Statement

1.1 The HKKA, as a Data User, respects personal data privacy and is committed to fully implementing and complying with the data protection principles and all relevant provisions of the Personal Data (Privacy) Ordinance (Cap. 486) and the Code of Practice issued by the Privacy Commissioner for Personal Data ("PCPD"). The HKKA is committed to ensuring that all its Executive Committee Members, Senate Members, Committee Members, staff and members uphold these obligations. The HKKA undertakes to:

(a) collect personal data directly related to the functions and activities of the HKKA only for lawful purposes, and by lawful and fair means;

(b) take all reasonably practicable steps to ensure that personal data are accurate, up-to-date and kept no longer than necessary;

(c) use the personal data collected only for the purposes, or directly related purposes, for which the data were to be used at the time of collection, unless the Data Subject concerned has given consent to a change of use or such use is permitted by law;

(d) take all reasonably practicable steps to ensure that personal data are protected against unauthorised or accidental access, processing, erasure or other use, consistent with the HKKA Guidelines and Procedures on Information Security and the HKKA Incident Response Procedure;

(e) take all reasonably practicable steps to ensure that the public is informed of the kinds of personal data that the HKKA holds and the purposes for which the data are to be used; and

(f) permit Data Subjects to access and correct their personal data, and process data access and correction requests in a manner permitted or required by law.

2. Types of Personal Data Processed by the HKKA

2.1 In the course of its operations, the HKKA may process the following types of personal data of Executive Committee Members, Senate Members, Committee Members, staff, athletes, coaches, referees, participants and other individuals:

(a) identification data (e.g. name and Hong Kong Identity Card / passport details);

(b) personal details (e.g. age, sex, date of birth, marital status, occupation, address, telephone number, email address and other contact details);

(c) employment records (e.g. job applications, past and present staff's job particulars, details of salary, payments, benefits, leave, training records, group medical and dental insurance records, mandatory provident fund schemes, performance appraisals, and disciplinary matters);

(d) payment details (e.g. bank or credit card details, for enrolment in events or activities);

(e) health information (e.g. data from medical tests and emergency contact details);

(f) vehicle information; and

(g) images (e.g. photographs of an individual participating in the HKKA's events or activities).

3. Main Purposes for Processing Personal Data

3.1 The purposes for which the HKKA processes personal data include:

(a) to verify an individual's identity;

(b) to ensure compliance with the rules and regulations of the HKKA and of international sports governing bodies;

(c) to maintain and develop services, including programmes, activities and events;

(d) to enable athletes and Executive Committee Members to participate in international multi-sports Games, including the selection of potential athletes into the Hong Kong, China Delegation;

(e) to organise, conduct and promote the HKKA's events and activities;

(f) to maintain relationships with the HKKA's members;

(g) to handle complaints or enquiries as appropriate, in accordance with the HKKA Guidelines and Procedures on Handling of Complaints and the HKKA Guidelines and Procedures on Appeals;

(h) to carry out surveys and statistical analyses;

(i) for purposes related to recruitment of staff, manpower management, and maintenance of the employment relationship;

(j) for security purposes, in accordance with the HKKA Guidelines and Procedures on Information Security; and

(k) where otherwise reasonably necessary for the HKKA to carry out its functions.

4. Lawful Basis for Processing Personal Data

4.1 The HKKA only processes personal data where there is a lawful basis for doing so, namely:

(a) Consent: the Data Subject has given clear consent for the HKKA to process their personal data for a specific purpose;

(b) Contract: the processing is necessary for a contract the HKKA has with a Data Subject, or because a Data Subject has asked the HKKA to take specific steps before entering into a contract;

(c) Legal obligation: the processing is necessary for the HKKA to comply with the law;

(d) Vital interests: the processing is necessary to protect the Data Subject's life;

(e) Public task: the processing is necessary for the HKKA to perform a task in the public interest; and

(f) Legitimate interests: the processing is necessary for the legitimate interests of the HKKA or of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.2 The HKKA will, on occasion, need to process special category personal data (e.g. when conducting medical or anti-doping tests) or criminal record information (e.g. when carrying out No Criminal Conviction Record or Sexual Conviction Record Checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required.

5. How the HKKA Collects Personal Data

5.1 Generally, the HKKA collects personal data from the individual directly. This may be via a form, an online platform, or in the ordinary course of interaction or communication.

5.2 In some cases, personal data may be supplied by third parties (e.g. other professionals or authorities working with that individual) or collected from publicly available resources.

5.3 The HKKA will not collect personal data from a minor without the prior consent of a person with parental responsibility for the minor.

6. Access to and Sharing of Personal Data

6.1 For the most part, personal data collected by the HKKA remains within the HKKA and is processed by appropriate individuals on a "need-to-know" basis.

6.2 Some of the HKKA's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. All such service providers are bound by a contractual duty to keep confidential any data they come into contact with, and to protect it against unauthorised access, use and retention.

6.3 Where necessary, the HKKA may be required to share personal data with third parties, such as:

(a) professional advisers (e.g. lawyers, insurers and auditors);

(b) government authorities;

(c) partners or related organisations (e.g. the Sports Federation & Olympic Committee of Hong Kong, China, the International Olympic Committee, or the Organizing Committee of a multi-sports Games); and

(d) where appropriate, parties who will be contacted by the HKKA in the handling of a complaint or appeal under the HKKA Guidelines and Procedures on Handling of Complaints or the HKKA Guidelines and Procedures on Appeals, including the party being complained against and other parties concerned.

6.4 Personal data held by the HKKA will not be disclosed to third parties unless the disclosure is for the purpose for which the data was to be used at the time of its collection, or a directly related purpose, or with the express and voluntary consent of the Data Subject, unless the obtaining of such consent is exempted under the law.

6.5 Unnecessary and excessive disclosure of personal data shall not be made. For example, in issuing documents relating to a complaint, enquiry or disciplinary matter under the HKKA Guidelines and Procedures on Handling of Complaints or the HKKA Guidelines and Procedures on Appeals, unnecessary personal data shall be removed or redacted.

7. Information Collected on the HKKA's Websites

A cookie is a small amount of data created on a computer when a person visits a website. It often includes an anonymous unique identifier and can be used to identify a computer. Cookies are used by the HKKA to collect statistics about the number of visits to the HKKA's websites and users' preferences for websites and online services. Users may choose to accept or reject cookies; if a user rejects cookies, some functions of the website (such as saving preferences or accessing certain online services) may not be available.

When a user visits the HKKA's websites, the webserver makes a record of the visit, including the user's IP address (and domain name), the type and configuration of browser used, language settings, general location, operating system, previous sites visited, and the time, duration and pages visited (webserver access log). The HKKA uses the webserver access log only for the purpose of maintaining and improving its websites (for example, to determine the optimal screen resolution or which pages are most frequently visited), and does not use, and has no intention of using, such data to personally identify anyone.

8. Protection Measures

The HKKA shall take appropriate steps to protect the personal data it holds against loss, unauthorised access, use, modification or disclosure, including training on personal data protection for staff who handle personal data in their daily work, and the measures set out in the HKKA Guidelines and Procedures on Information Security and the HKKA Incident Response Procedure.

9. Retention

Personal data will not be kept longer than is necessary to fulfil the purpose for which it was collected. Personal data that is no longer needed is either irreversibly anonymised (and the anonymised information retained) or securely destroyed. The table below sets out the HKKA's recommended maximum retention periods for the principal categories of personal data it holds.

Category	**Type of personal data**	**Maximum retention period**
Events / Programmes	Personal data of past participants	7 years from completion of the event or programme
Multi-sports Games	Personal data of Delegation members	8 years from completion of the Games, in accordance with the Financial Guidelines of Olympic Solidarity
Membership	Personal data of past individual members / representatives of Member associations	7 years from the date of cessation of membership or representation

Category	Type of personal data	Maximum retention period
Employment records	Job applications of unsuccessful candidates	2 years from completion of the recruitment exercise
Employment records	Personal files of past employees	7 years from the date of cessation of employment
Complaints	Personal data of complainants / complainees under the HKKA Guidelines and Procedures on Handling of Complaints	7 years from completion of the complaint, after which all related personal data shall be deleted or anonymised (unless a longer period is required by an applicable statutory or regulatory requirement)
Appeals	Personal data of appellants under the HKKA Guidelines and Procedures on Appeals	7 years from conclusion of the appeal, after which all related personal data shall be deleted or anonymised (unless a longer period is required by an applicable statutory or regulatory requirement)

The Executive Committee should ensure that personal data is not kept longer than necessary to fulfil the purpose for which it is used, and should keep a personal data inventory to track the types of personal data it holds and how that data is processed. As a matter of good practice, personal data not collected directly by the HKKA but transferred from another source should be disposed of properly immediately after use, and fresh data requested each time it is required.

10. Data Access and Correction

10.1 Data access requests should be made in writing, using the form prescribed by the PCPD, and sent to the Data Protection Officer (see section 13.6 below) in person or by fax, email or post.

10.2 When handling a data access or correction request, the HKKA will check the identity of the requester to ensure that he or she is the person legally entitled to make the request.

11. Code of Practice on Data Protection

The HKKA should devise a Code of Practice on Data Protection, which provides guidance and good practice in safeguarding personal data privacy, and shall ensure that it is made known to all persons within the scope of this document.

12. Definition of Personal Data

“Personal data” refers to information that relates to a living person and can be used to identify that person, and which exists in a form in which access to, or processing of, the data is practicable. Examples of personal data protected under the Ordinance include names, phone numbers, addresses, identity card numbers, photographs, medical records and employment records.

13. Six Data Protection Principles

The PCPD recognises six Data Protection Principles ("DPPs") that represent the core of the Ordinance: DPP1 (Collection – Purpose and Means); DPP2 (Accuracy and Retention); DPP3 (Use of Data); DPP4 (Security); DPP5 (Openness); and DPP6 (Data Access and Correction). The following paragraphs provide practical guidance on how the HKKA adheres to the six DPPs.

13.1 Collection: Purpose and Means (DPP1)

(a) The purpose of collection must be directly related to the functions or activities of the HKKA, and the data collected for a specified purpose should be adequate but not excessive.

(b) During collection, Data Subjects should be informed explicitly of: the purpose for which the data is collected; the parties to whom the data may be transferred; whether it is obligatory or voluntary to supply the data, and the consequences of not doing so; the Data Subject's rights to request access to and correction of the data held by the HKKA; and the person to be contacted for data access and correction.

(c) A Personal Information Collection Statement ("PICS") should be included when collecting personal data directly from a Data Subject. Appendix I lists circumstances under which a PICS is, or is not, required; a sample PICS is at Appendix II.

(d) When proposing to collect Hong Kong Identity Card numbers or copies, consideration should be given to less privacy-intrusive alternatives (e.g. collecting only the first four digits, or using a staff card or other photo identification instead). Reference should be made to the relevant Code of Practice issued by the PCPD.

13.2 Accuracy and Retention (DPP2)

(a) The HKKA should review and update the personal data it holds periodically to ensure accuracy. Inaccurate data, and data no longer in use, should be deleted.

(b) The HKKA should keep a personal data inventory to track the types of personal data it holds and how that data is processed.

(c) The Executive Committee should ensure that personal data is not kept longer than necessary, in accordance with the retention table at section 9 above.

(d) As good practice, personal data not collected directly by the HKKA but transferred from another source should be disposed of properly immediately after use.

13.3 Use of Data (DPP3)

(a) Personal data must be used for the purpose for which it was collected, or a directly related purpose, unless voluntary and explicit consent is obtained from the Data Subject for a new purpose.

(b) Unnecessary and excessive disclosure of personal data should not be made (for example, in issuing documents relating to a complaint or disciplinary matter, the Executive Committee should remove or redact unnecessary personal data).

(c) When personal data is transferred to another party, the transferor should remind the receiving party to handle it with an appropriate level of confidentiality and to use it only for the agreed purpose.

(d) In direct marketing (e.g. promoting programmes or activities, or soliciting donations), written or verbal consent must be obtained from the Data Subject; if only verbal

consent is obtained, a written confirmation (stating the date of consent, the permitted types of personal data, and the permitted class of marketing subjects) should be issued within 14 days.

(e) Valid consent is not obtained if a Data Subject refuses to provide contact information (so that the written confirmation cannot be sent), or if the written confirmation is returned undelivered.

13.4 Security (DPP4)

The Executive Committee should take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or other use, including the following measures, and consistent with the HKKA Guidelines and Procedures on Information Security:

Access control: personal data should be disseminated to another party only if necessary, on a "need to know" and "need to use" basis (for example, a staff member's access to personnel records should cease immediately upon transfer to another post); measures must be in place to ensure the integrity, prudence and competence of authorised persons; personal data should not be taken away from the office save in special circumstances; and where a data processor (e.g. a service provider) is engaged, contractual or other means must be adopted to prevent unauthorised or accidental access, processing, erasure, loss or use.

Data storage: an appropriate physical location should be identified for safe storage (e.g. lockable filing cabinets or rooms with controlled access); files should not be left open where they can be seen by unauthorised persons; personal or sensitive data should generally not be stored on portable devices, and where this is unavoidable, only the minimum necessary data should be stored, it should be password-protected, and deleted as soon as the task for which it is required is complete.

Data transmission: appropriate measures should be adopted to ensure secure transmission (e.g. documents containing personal data sent by post should be sealed and marked "private and confidential"); shared drives should be used where available; personal or sensitive data sent electronically should be password-protected, with email addresses and attachments double-checked; and BCC or mail merge should be used for mass emails to avoid disclosing recipients' email addresses.

Data disposal: personal data should be disposed of properly after the applicable retention period (e.g. hard copy documents shredded, and disks or memory sticks formatted or destroyed).

Other: information that could lead to identification of a Data Subject in statistical analysis should be anonymised.

13.5 Openness (DPP5)

The HKKA will make available to stakeholders: the personal data policies and practices it has adopted; the types of personal data it holds; and the purposes for which the personal data is used or to be used.

13.6 Data Access and Correction (DPP6)

(a) A Data Subject must be given access to his or her own personal data, and allowed to make corrections if it is inaccurate. A data access request is a request made by an individual asking the HKKA to inform him or her whether it holds personal data of which the individual is the Data Subject, and if so, to supply a copy of that data.

(b) Data Subjects are encouraged to make data access requests using the form prescribed by the PCPD.

(c) Data access requests shall be processed by a Data Protection Officer ("DPO"), designated by the Executive Committee, who has undergone appropriate training. On

receiving a request, the DPO should ascertain the identity of the requester and assess whether the HKKA holds the relevant personal data.

(d) If the HKKA holds the relevant personal data, a copy shall be supplied to the Data Subject within 40 calendar days of receiving the request. If the HKKA does not hold the requested data, the requester shall still be informed in writing within the same 40-day period.

(e) The HKKA may impose a fee for complying with a data access request, which shall not be excessive.

(f) The HKKA may refuse to comply with a data access request if: it is not supplied with sufficient information to identify the requester; it cannot comply without disclosing the personal data of a third party; or compliance is for the time being prohibited under the Ordinance or another ordinance.

(g) A log book shall be kept to register all data access requests for the past 6 years, stating reasons for any refusal.

1. Opt-out Requests

1.1 A Data Subject may, at any time, require the HKKA to cease using his or her personal data for direct marketing. Such requests may be made verbally or in writing.

1.2 To comply with an opt-out request, staff involved in direct marketing should maintain an opt-out list of all persons who have indicated that they do not wish to receive further marketing approaches.

2. Handling of a Data Breach

A data breach affecting personal data is handled in accordance with this section and the HKKA Incident Response Procedure, which sets out the escalation and containment steps for a security incident more generally.

2.1 In case of a data breach, the incident should be reported to the DPO and the Executive Committee in the first instance, and essential information relating to the breach should be gathered.

2.2 The following parties may also be notified as appropriate: law enforcement agencies; the PCPD; and IT experts (including, where engaged, the Incident Coordinator referred to in the HKKA Incident Response Procedure).

2.3 Measures should be adopted to contain the breach (e.g. suspension of a system function or access right), and an assessment made of the potential damage and harm caused.

2.4 Consideration should be given to notifying affected Data Subjects and relevant parties. Where Data Subjects are not immediately identifiable, or where the public interest so requires, public notification through the HKKA's website or the media may be considered.

2.5 A thorough investigation into the breach should be carried out, with the results reported to the Executive Committee and kept in a detailed report, and areas for improvement identified to prevent recurrence.

2.6 The Data Breach Information Sheet at Appendix III should be used to consolidate information relating to the breach, record remedial actions taken, and conduct a post-incident review.

3. **Enquiries**

The Kendo Association of Hong Kong, China

Address: Room 1029, Olympic House, 1 Stadium Path, So Kon Po, Hong Kong

Tel: +852 2504 8445

E-mail: hkka@hongkongkendo.com

APPENDIX I: CIRCUMSTANCES UNDER WHICH A PICS IS / IS NOT REQUIRED

Scenario	PICS required	PICS not required
Event registration	Personal data is collected directly from participants.	Personal data of corporate team participants is provided by the organisation they represent.
Staff recruitment	Personal data is collected directly from job applicants.	N/A
Membership programme	Personal data is collected directly from members.	N/A
Lucky draw	Contact details are collected directly from participants.	N/A
Athletes Committee election	Personal data is collected directly from candidates or voters.	Personal data of candidates or voters is provided by the HKKA.
Multi-sports Games	N/A	Personal data of delegation members is provided by the HKKA.

This list is for reference only and is not exhaustive. If in doubt, advice should be sought when deciding whether a PICS is required in a particular case.

APPENDIX II: PERSONAL INFORMATION COLLECTION STATEMENT (SAMPLE)

1. The personal data collected is used by the HKKA for [purpose] or other directly related purpose(s).

2. Please note that it is mandatory to provide the personal data marked with an asterisk. If you do not provide such data, the HKKA may not be able to provide you with [service].

3. Your personal data held by the HKKA will be kept confidential within the retention period set out in the HKKA Guidelines and Procedures on Personal Data Privacy Protection, but may be shared with other parties, including [other organisations], for the purpose(s) stated above.

4. In accordance with the Personal Data (Privacy) Ordinance, you have the right to access, amend, and request a copy of your personal data held by the HKKA. Requests may be made to the Data Protection Officer in writing, by email to [email address] or by post to [mailing address]. A fee of $[x] per A4-size page may be charged to cover the administrative cost.

5. For further details, please refer to the HKKA Guidelines and Procedures on Personal Data Privacy Protection at [link].

APPENDIX III: DATA BREACH INFORMATION SHEET

Date and time breach discovered:	
Reported by:	
Description of the breach:	
Systems / data affected (including whether personal data is involved):	
Immediate containment action taken:	
Parties notified (e.g. PCPD, law enforcement, IT experts, affected Data Subjects) and date:	
Root cause identified:	
Remedial action taken / planned:	
Reviewed by (Data Protection Officer / Executive Committee) and date:	