

Shuttlecock Association of Hong Kong, China

Guidelines and Procedures on Personal Data Privacy Protection

Issued in compliance with the Personal Data (Privacy) Ordinance (Cap. 486) and the requirements of the Leisure and Cultural Services Department under the Sports Subvention Scheme

Document Ref.	Version	Effective Date	Approved by
SAHKC/PDP/01	1.0	1 January 2027	Executive Committee

1. Purpose

These Guidelines set out how the Association collects, holds, uses and protects personal data. They give effect to the six Data Protection Principles (DPPs) in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486) (the "Ordinance") and support the Association's accountability for the public funds it receives.

2. Scope

These Guidelines apply to all staff, Executive Committee members, coaches, team officials, volunteers and contractors of the Association (collectively "staff") who handle personal data in any form — paper, electronic, photographic or video.

Personal data handled by the Association typically includes: member and athlete registration records; identity document and date-of-birth data; contact details; emergency contacts; parent or guardian details for minors; medical, injury and anti-doping information; coaching and qualification records; bank and payment details; and employment records.

3. Responsibilities

Role	Responsibility
Executive Committee	Approves these Guidelines; oversees compliance; reviews reported data breaches.
Data Protection Officer (DPO)	Appointed by the Executive Committee (in practice the Secretary General or his/her delegate). Day-to-day owner of these Guidelines; handles data access and correction requests, enquiries, complaints and breach reporting; arranges annual staff briefing.
All staff	Comply with these Guidelines; collect and use personal data only as required for their duties; report any suspected breach to the DPO immediately.

4. Guidelines — the Six Data Protection Principles

DPP1 — Collection

- Collect personal data only for a lawful purpose directly related to the Association's activities, and only what is necessary and adequate but not excessive for that purpose.

- Collect by lawful and fair means. Do not collect Hong Kong Identity Card numbers or copies unless there is a genuine need (e.g. competition eligibility verification, employment, insurance).
- Provide a Personal Information Collection Statement (PICS) on every form (paper or online) at or before collection, stating: the purpose of collection; whether supply is obligatory and the consequence of not supplying; the classes of persons to whom the data may be transferred; and the right to request access and correction with the DPO's contact details.
- For members under 18, obtain the written consent of a parent or guardian.

DPP2 — Accuracy and Retention

- Take all practicable steps to keep personal data accurate and up to date; invite members to update their records at each annual renewal.
- Do not keep personal data longer than necessary. Follow the retention schedule at Section 6.
- Where a data processor (e.g. an IT vendor or event contractor) is engaged, use contractual means to ensure it does not keep the data longer than necessary and protects it adequately.

DPP3 — Use

- Use personal data only for the purpose stated at collection or a directly related purpose.
- Any new use, or disclosure to a third party not covered by the PICS, requires the express and voluntary consent of the individual (prescribed consent), obtained in writing and filed.
- Do not use personal data for direct marketing (including sponsor promotions) unless the individual has been notified of the data and marketing classes involved and has given consent. Provide an opt-out channel in every marketing message and act on opt-outs without charge.

DPP4 — Security

- Access on a need-to-know basis only; access rights are approved by the DPO and reviewed at least annually.
- Lock paper records in cabinets; store electronic records on the Association's approved systems with individual accounts and strong passwords.
- Encrypt or password-protect personal data before sending it by email or carrying it outside the office; send the password separately.
- Dispose of records securely by shredding (paper) or secure deletion (electronic).
- Refer to the Association's Guidelines and Procedures on Information Security for the detailed technical controls.

DPP5 — Openness

- Publish a Privacy Policy Statement on the Association's website setting out the kinds of personal data held and the Association's policies and practices on handling them.
- Make these Guidelines available to all staff.

DPP6 — Access and Correction

- Individuals may request a copy of their personal data and request correction of inaccurate data.
- Comply with, or refuse with written reasons, a data access or correction request within 40 calendar days of receipt.
- A reasonable, not excessive, fee may be charged for complying with a data access request.

5. Procedures

5.1 Handling a Data Access or Correction Request

- Step 1 — Forward the request to the DPO on the day it is received. Requests may be made on the form specified by the Privacy Commissioner (Form OPS003) or in writing.
- Step 2 — The DPO verifies the requestor's identity and logs the request in the Data Request Register (date received, requestor, nature, due date).
- Step 3 — The DPO retrieves the data, redacts any third-party personal data, and prepares the reply.
- Step 4 — The DPO issues the reply within 40 days. If the request is refused, state the reason and the relevant exemption in writing and record it in the Register.
- Step 5 — For a correction request, correct the data and notify any third party to whom the incorrect data was disclosed in the previous 12 months.

5.2 Handling a Data Breach

- Step 1 — Report: any staff member who discovers or suspects loss, theft, unauthorised access to or disclosure of personal data must inform the DPO immediately and in any event within 24 hours.
- Step 2 — Contain: the DPO stops the breach (e.g. suspend the account, recover or remotely wipe the device, take the system offline) and preserves evidence.
- Step 3 — Assess: the DPO assesses the data involved, the number of individuals affected and the risk of harm.
- Step 4 — Notify: where there is a real risk of harm, notify the affected individuals as soon as practicable and notify the Office of the Privacy Commissioner for Personal Data (PCPD) using its Data Breach Notification Form. Notify the Police where a crime is suspected, and inform LCSD where the breach affects subvented programmes.
- Step 5 — Review: the DPO reports the breach and the remedial actions taken to the Executive Committee at its next meeting, and updates these Guidelines where needed.

5.3 Engaging Contractors and Service Providers

- Before transferring personal data to any contractor (IT vendor, event organiser, cloud service, insurer), the DPO must ensure the written contract requires the contractor to: use the data only as instructed; apply adequate security measures; not sub-contract without consent; return or delete the data on completion; and report any breach to the Association immediately.

5.4 Training and Monitoring

- All new staff receive a briefing on these Guidelines within one month of joining and sign the Acknowledgement at the Annex.
- All staff attend a refresher briefing at least once a year.
- The DPO carries out an annual self-check of personal data holdings, forms, retention and access rights, and reports the results to the Executive Committee.

6. Retention Schedule

Record	Retention period
Member / athlete registration records	7 years after membership ends
Competition entry and result records	7 years (results of record may be kept permanently in anonymised form)
Medical, injury and anti-doping records	As required by the applicable anti-doping rules; otherwise

	7 years
Records relating to minors	Until 7 years after the individual reaches 18
Employment records (staff and coaches)	7 years after employment ends
Unsuccessful job applications	2 years
CCTV / event photographs and video	1 year unless required for a specific purpose
Subvention-related records	As required by the LCSD subvention agreement (not less than 7 years)

Records are destroyed securely on expiry of the period above unless they are required for an ongoing legal, audit or disciplinary matter.

7. Non-compliance

Failure to comply with these Guidelines may result in disciplinary action. A contravention of the Ordinance may lead to an enforcement notice, prosecution and a claim for compensation against the Association or the individual concerned.

8. Review

The DPO reviews these Guidelines at least every two years, or earlier following a data breach, a change in the law, or a change in LCSD requirements. Revisions are approved by the Executive Committee.

9. References

- Personal Data (Privacy) Ordinance (Cap. 486), Schedule 1 — Six Data Protection Principles
- PCPD, "Guidance on Data Breach Handling and Data Breach Notifications"
- PCPD, "Guidance Note on Data Security Measures for Information and Communications Technology" (2022)
- PCPD, "Privacy Management Programme: A Best Practice Guide"
- LCSD Sports Subvention Scheme — subvention agreement and corporate governance requirements

Enquiries: Data Protection Officer, Shuttlecock Association of Hong Kong, China. PCPD Hotline: 2827 2827 / www.pcpd.org.hk

Annex — Staff Acknowledgement

I confirm that I have read and understood the Guidelines and Procedures on Personal Data Privacy Protection, and I agree to comply with it in the course of my duties with Shuttlecock Association of Hong Kong, China. I understand that non-compliance may lead to disciplinary action and, where the law is breached, to legal liability.

Name	Position	Signature	Date