保護個人資料政策
Policy on Personal Data Privacy Protection

目的 Objective
根據《個人資料（私隱）條例》（第 486 章），建立一個尊重個人資料私隱、 遵守保障資料原則的環境。
To demonstrate commitment in respecting personal data privacy, complying with data protection principles and all relevant provisions of the Personal Data (Privacy) Ordinance (Cap. 486).

本政策適用於所有董事、委員會成員、職員（包括短期合約和非全職職員）、 會員、運動員、教練、裁判員、以及參與體育總會業務、活動或比賽的每個人。
It applies to all Executive Committee members, Committee Members, and staff irrespective of their terms of employment, i.e., including short-term contract or part-time staff, members, athletes, coaches, umpires, and every person involved in the Association's business, activities, competitions, matches or events.

私隱政策聲明 Privacy Policy Statement
協會作為資料使用者，尊重個人資料私隱，並全力實施及遵守《個人資料 （私隱）條例》（第 486 章）及個人資料私隱專員發出的《實務守則》中保障資料原則以及各項有關規定。協會同樣致力於確保所有董事、委員會成員、職員和會員履行有關責任。協會承諾：
The Association, 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 Code of Practice issued by the Privacy Commissioner for Personal Data. The Association is equally committed to ensuring that all its Executive Committee Members, Committee Members, staff and members uphold these obligations. The Association undertakes to:

- 為直接與其職能或活動有關的合法目的，收集個人資料；
  Collect personal data directly related to the functions and activities of the Association only for lawful purposes, and by lawful and fair means;
- 採取所有切實可行的步驟，以確保持有的個人資料準確無誤，而保留時間不超過達致原來目的實際所需；
  Take all reasonably practicable steps to ensure that personal data are accurate, up-to-date and kept no longer than necessary;
- 除非得到資料當事人自願給予的明示同意，否則個人資料不得用於「新目的」，即原先收集資料時擬使用或相關的目的以外的目的；
  Use the personal data collected only for 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;

- 採取一切切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用；

  Take all reasonably practicable steps to ensure that personal data are protected against unauthorized or accidental access, processing, erasure or other use;

- 採取一切切實可行的步驟，告知資料使用者所持有的個人資料種類和使用於甚麼主要目的；和

  Take all reasonably practicable steps to ensure that the public is informed of the kinds of personal data that the Association holds and the purposes for which the data are to be used; and

- 允許資料當事人查閱及改正自己的個人資料。

  Permit Data Subjects to access and correct their personal data and process the data access/correction requests in a manner permitted or required by law.

處理個人資料類型 Types of Personal Data Processed by the Association

協會在其運作過程中，可能會處理以下類型的個人資料，包括執行委員、委員會成員、職員、運動員、教練、裁判員、參加者及其他人士的：

The Association, in the course of its operations, may process the following types of personal data of Executive Committee Members, Committee Members, staff, athletes, coaches, umpires, participants and other individuals:

- 身份資料（例如姓名和香港身分證/護照）Identification data (e.g., name and Hong Kong Identity Card/passport details)；
- 個人詳細資料（例如年齡、性別、出生日期、婚姻狀況、職業、地址、電話號碼、電郵地址和其他聯繫方式）
- Personal details (e.g., age, sex, date of birth, marital status, occupation, address, telephone number, email address and other contact details)；
- 僱傭記錄（例如工作申請、現有及過往的工作詳情、薪金、酬勞、福利、休假、培訓記錄、團體醫療及牙科保險記錄、強制性公積金計劃、工作表現評核及紀律事項等）Employment record (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)；
- 支付的詳細資料（例如銀行/信用卡的詳細資料等）Payment details (e.g., bank/credit card details)；
- 健康資訊（例如醫療檢查數據、級別鑑定資料、藥物使用清單及緊急聯絡方式）Health information (e.g., data from medical tests and emergency contact details)；
- 車輛資訊；和 Vehicle information; and

- 錄像和圖像（例如參與協會活動/項目的照片、影片和聲音記錄等）Videos and Images (e.g., video, photo and audio record of an individual participating in Association's events/activities)。

個人資料的處理目的 Main Purposes for Processing Personal Data

協會處理個人資料的目的如下：

The purposes for which the NSA processes personal data are:

- 核實個人身份 To verify an individual's identity；
- 確保遵從協會及國際體育管治機構的規則和條例 To ensure compliance with the rules and regulations of the Association and that of international sports governing bodies；
- 維持和發展不同的服務，包括項目、活動和賽事 To maintain and develop services, including programs, activities, and events；
- 協助運動員和執行委員參加國際綜合運動會 To enable athletes and Executive Committee Members to participate in international multi-sports Games；
- 組織、舉辦和促進體育總會的活動/賽事To organize, conduct and promote the Association's events/activities；
- 維持與協會會員的關係To maintain relationships with the NSA's members；
- 適當地處理投訴/查詢 To handle complaints/enquiries as appropriate；
- 進行調查、統計及數據分析 To carry out surveys and statistical analyses；
- 用於招聘工作人員、管理人力資源及維持僱傭關係 For purposes related to recruitment of staff, manpower management, and maintenance of employment relationship；
- 出於安全目的；和 For security purposes; and
- 任何其他協會因履行職能的合理原因 Where otherwise reasonably necessary for the NSA to carry out its functions。

處理個人資料的法律依據 Lawful Basis for Processing Personal Data

協會只在有合法依據的情況下處理個人資料：

The Association only processes personal data where there is a lawful basis for doing so.

- 資料當事人明確同意協會可為特定目的處理其個人資料 The Data Subject has given clear consent for the Association to process their personal data for a specific purpose；
- 是資料當事人與協會簽訂合約為前提，所採取的必要步驟 The processing is necessary for a contract the Association has with a Data Subject, or because a Data Subject has asked the Association to take specific steps before entering into a contract；
- 協會基於法律的要求 The processing is necessary for the Association to comply

with the law；

- 為了保障資料當事人的生命安全 The processing is necessary to protect the Data Subject's life；
- 為保障公衆利益而必需提供；和 The processing is necessary for the NSA to perform a task in the public interest; and
- 維護協會或第三方的法律權益而言，是必需而且必要的。除非有充分的理由，保護使用者/用戶/資料當事人的個人數據的重要性凌駕 於此類權益之上 The processing is necessary for the Association's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests。

在特定情況，基於法律所要求的責任或義務，協會或許需要處理特殊類別的個人資料（例如根據相關的機構的規定或要求，進行相應的醫學/運動禁藥測試時）；或犯罪記錄資料（例如進行無犯罪記錄/性犯罪記錄查核時）。 這同時包括，保護個人私隱和保障僱傭關係，根據法例的要求，同意交出個人資料。

In addition, the Association will on occasion need to process special category personal data (e.g., when conducting medical/anti-doping tests) or criminal records information (e.g., when carrying out No Criminal/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.

<u>如何收集個人資料 How the NSA Collects Personal Data</u>

- 一般而言，協會可以直接向個人用戶收集個人資料。可能通過表格、線上平台或在日常互動或交流中獲取。

  Generally, the Association collects personal data from the individual directly. This may be via a form, an online platform or simply in the ordinary course of interaction or communication.
- 某些情況下，個人資料可能由第三方提供（例如，其他專業人士或相關部門）或取自其他公共資源。

  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.
- 未經未成年人的父母或監護人同意前，體育總會不會未成年人收集個人資料。

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

<u>存取和共享個人資料 Access to and Sharing of Personal Data</u>

- 協會收集的個人資料大部分將儲存/保留在協會內，並由適當的人員基於「需

要知道」的原則作出妥善處理及保管。

For the most part, personal data collected by the Association will remain within the Association and will be processed by appropriate individuals on a "need-to-know" basis.

- 協會所舉辦的部分活動是由第三方代表執行，如資訊系統、網頁開發商或雲端存儲供應商。所有協會的服務供應商均受合約條款及義務約束，確保他們接觸到的一切數據/資料得以保密，以防止未經授權的接觸、使用和儲存。

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

- 體育總會可能需要與以下第三方共享個人資料：

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

  - 專業顧問（例如律師、保險公司和審計師）Professional advisers (e.g., lawyers, insurers and auditors)；
  - 政府部門 Government authorities；
  - 合作夥伴或相關組織（例如港協暨奧委會、中國香港殘疾人奧委會、國際殘疾人奧林匹克委員會、綜合性運動會籌備委員會等）；和 Partners or related organizations (e.g., Sports Federation & Olympic Committee of Hong Kong, China, China Hong Kong Paralympic Committee, International Paralympic Committee, Organizing Committee of multi-sports Games); and
  - 在適當情況下，協會在處理投訴/查詢案件期間將會聯繫的各方，包括被投訴人和/或任何有關人士 Where appropriate, parties who will be contacted by the Association during the handling of a complaint/enquiry case including the party being complained against and/or other parties concerned。

- 協會持有的個人資料將不會被披露給第三方，除非是原先收集資料時擬使用或直接相關的目的，或得到資料當事人自願給予的明示同意。

  Personal data held by the Association 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 collection of the data or a directly related purpose, or with the express consent of the data subject given voluntarily unless the obtaining of such consent is exempted under the law.

- 協會不會作出不必要和過度的個人資料披露，例如與投訴/查詢案件或紀律事項有關的文件其中不必要的個人資料將被刪除和編輯。

  Unnecessary and excessive disclosure of personal data will not be made, e.g., in issuing documents in relation to complaint/enquiry case or disciplinary matters, unnecessary personal data will be removed and redacted.

協會網站上收集的資訊 Information Collected on the Association's Websites

- 當使用者使用電腦瀏覽網站時，小型文字檔案（Cookies）會建立於電腦內。小型文字檔案通常包含一個匿名而獨有的標識符，用以識別個別電腦。協會使用 Cookie 來收集用戶存取其網站的次數，以及用戶對協會網站的使用偏好及其他網絡服務的數據。用戶可以選擇接受或拒絕 Cookie。如果用戶拒絕 Cookie，他們或將無法使用網站的某些功能，例如儲存個人偏好選項和存取部 分線上服務。

  A cookie is a small amount of data created in a computer when a person visits a website on the computer. It often includes an anonymous unique identifier. A cookie can be used to identify a computer. Cookies are used by the Association to collect statistics about the number of visits of users to the Association's websites and the users' preference of websites and online services offered on the Association's websites. Users may choose to accept or reject cookies. If users reject cookies, they will not be able to use some of the functions of the websites, such as saving preferences and accessing some online services.

- 當用戶瀏覽協會的網站時，網絡伺服器會儲存相關記錄，包括用戶的 IP 地址（及網域名稱）、瀏覽器類型及配置、語言設定、地理位置、操作系統、先前瀏覽的網頁以及之前瀏覽相關的網頁所逗留的時間和曾到訪網站的頁面（網絡伺服器存取日誌）。協會使用網絡伺服器的存取日誌來維護和改進本會的網站，例如決定最佳屏幕分辨率，以及最常瀏覽的頁面等。協會僅會將此類數據用於網站改進及優化網站服務。協會不會使用，也無意使用使用者的數據來識別任何人的個人身份。

  When a user visits the Association's websites, the webserver makes a record of the visit that includes the user's IP addresses (and domain names), the types and configurations of browsers, language settings, geo-locations, operating systems, previous sites visited, and time/duration and the pages visited (webserver access log). The Association uses the webserver access log for the purpose of maintaining and improving its websites such as to determine the optimal screen resolution, which pages have been most frequently visited etc. The Association uses such data only for website enhancement and optimization purposes. The Association does not use, and have no intention of using the visitor data to personally identify anyone.

六項保障資料原則 Six Data Protection Principles

個人資料私隱專員訂明以下六項保障資料原則，這些原則代表了條例的核心內容：

The Privacy Commissioner for Personal Data recognizes six Data Protection Principles (DPPs) that represent the core of the Ordinance:

原則 1 - 收集目的及方式

DPP1 - Collection - Purpose & Means

- 收集資料的目的必須直接與協會的職能或活動有關，收集到的資料應該充足但不超乎適度。

  The purpose of collection must be directly related to the functions or activities of the Association, and the data collected in relation to a specified purpose should be adequate but not excessive.

- 在收集個人資料時，資料當事人應明確被告知以下事項：

  During the collection of personal data, Data Subjects should be informed explicitly of the following:

  - 資料將用於甚麼目的 Purpose for which the data is collected；
  - 資料可能被轉移給甚麼類別人士 Parties to whom the data may be transferred；
  - 提供資料是否為強制或自願，以及不提供的後果 Whether it is obligatory or voluntary to supply the data, and the consequences of not doing so；
  - 資料當事人有權要求查閱及改正協會持有的資料的權利；和 Rights of the Data Subject to request access to and correction of the data held by the NSA; and
  - 負責資料查閱及改正的聯絡人 Person to be contacted for data access and correction。

- 當向個別人士收集個人資料時，應提供一份「收集個人資料聲明」。附件 1 載列了需要或不需要提供「收集個人資料聲明」的情況。「收集個人資料聲明」見附件 2。

  A Personal Information Collection Statement (PICS) should be included when collecting personal data directly from a Data Subject. Appendix I lists out some circumstances under which a PICS is or is not required. A form of PICS is shown at Appendix II.

- 當收集香港身份證號碼或副本時，應考慮採用不侵犯私隱的方法，例如收集身份證號碼的前四位數字以識別同名人士。亦可使用員工證或其他附有照片的證件代替身份證來核實身份。有關詳情請參考個人資料私隱專員公署發布的相關實務守則。

  When proposing to collect HKID card numbers or copies, consideration should be given to adopting other less privacy-intrusive alternatives, e.g., collecting the first four digits of HKID card numbers should be sufficient for the purpose of identification of persons with the same names. Staff cards or other photo identification documents could be used instead of HKID card to check the identity of a person. For further information, reference should be made to the relevant Code of Practice issued by the Office of the Privacy Commissioner for Personal Data.

原則 2 - 準確性及保留期限

DPP2 - Accuracy & Retention

- 協會需定期檢討和更新個人資料，確保資料的準確性。 不準確的資料應立即停止使用並刪除。

  The Association should review and update the personal data periodically to ensure that it is accurate. Inaccurate data and data no longer in use should be deleted.

- 協會需保存個人資料庫存，就個人資料進行定期檢討、修訂及更新。

  The Association should keep a personal data inventory to keep track of the types of personal data it holds and how the personal data is being processed.

- 確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或 會被使用於的目的所需的時間。

  Ensure that personal data is not kept longer than necessary to fulfil the purpose for which it is used.

- 遵行良好指引，如並非直接向資料當事人收集個人資料，而是使用第三方提供資料，則應在使用後立即妥善處理有關資料。每次使用時都應向資料提供方請求最新的資料。

  As a good practice, personal data not collected directly by the Association but transferred from another source should be disposed of properly immediately after use. Fresh data should be requested each time it is required.

- 下表列出了協會持有不同類別個人資料的建議最長保留期限：

  The below table shows the recommended maximum retention periods for different types of personal data held by the Association:

個人資料類別 Type of Personal Data		最長保留期 Maximum Retention Period
秘書處 Secretariat		
活動/項目 Events/Programs	參加者的個人資料 Personal data of past participants	活動/項目完成之日起計7年 7 years from the completion of the event/program
綜合性運動會 Multi-sports Games	代表團成員的個人資料 Personal data of Delegation members	從賽事完成之日起計 8 年 8 years from the completion of the Games
會員 Membership	過去個別會員/會員協會代表的個人資料	會員資格/代表資格終止之日起計 2 年

	Personal data of past individual members / representatives of Member Associations	2 years from the date of cessation of membership/representation
僱傭記錄 Employment record	落選的求職者的個人資料 Job applications of unsuccessful candidates	招聘工作完成之日起計 2 年 2 years from the completion of the recruitment exercise
	離職職員的個人檔案	離職日期起計 7 年
投訴 Complaints	投訴人/被投訴人的個人資料 Personal data of complainants / complainees	投訴完成後 2 年內，所有相關個人資料應被刪除或匿名化（除非有任何相關法律或監管要求 將資料保存更長時間） 2 years from the completion of the complaint, after which all related personal data shall be deleted or anonymized (unless there are any relevant statutory or regulatory requirements to keep the data for a longer period of time)

原則 3 - 資料的使用

DPP3 - Use of Data

- 個人資料必須用於收集資料的目的或直接相關的目的，除非得到資料當事人自願給予的訂明同意，否則個人資料不得用於新目的。

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

- 不應作出不必要和過度的個人資料披露，例如與投訴/查詢案件或紀律事項有關的文件，其中不必要的個人資料將被刪除和編輯。

  Unnecessary and excessive disclosure of personal data should not be made, e.g., in issuing documents in relation to complaint/enquiry case or disciplinary matters, the Association should not disclose unnecessary and excessive personal data and should

remove or redact the same.

- 當個人資料轉移給另一方時，轉移方應提醒承轉人以適當的機密級別處理該資料，並僅用於已同意的目的。

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

- 在直接促銷中（如宣傳項目/活動、索求捐贈/貢獻等）：

  In direct marketing (e.g., promoting programmes/activities, soliciting donations/contributions, etc.):

  - 必須獲得資料當事人的同意，才能使用其個人資料。資料當事人還應被明確告知，其個人資料擬在或在直接促銷中，就某類別的促銷標的而被使用。促銷同意書詳見附件 3。

    Written or verbal consent must be obtained from Data Subjects for the use of their personal data. Data Subjects should also be informed of the classes of marketing subjects in relation to which the Data Users are going to carry out direct marketing. A form of a consent for direct marketing is shown at Appendix III.

  - 如該項同意屬口頭同意，該資料使用者已自收到該項同意起計的 14 日內，向該當事人發出確認以下事宜的書面確認。

    If only verbal consent is obtained from a Data Subject, a written confirmation should be issued to the Data Subject within 14 days after the consent is received.

- 書面確認應包括：

  The written confirmation should include:

  - 收到同意的日期 Date of receipt of the consent；
  - 有關許可種類個人資料；及 Permitted types of personal data; and
  - 有關許可類別促銷標的 Permitted class of marketing subjects。

- 如果資料當事人拒絕提供聯絡資料而導致無法發送書面確認，或者發送給資料當事人的書面確認未送達而被退回，則視為未獲得有效同意。

  Valid consent is considered not obtained if a Data Subject refuses to provide his/her contact information and as a result the written confirmation could not be sent, or when the written confirmation sent to the Data Subject is returned undelivered.

原則 4 - 資料的保安

DPP4 - Security

協會將採取所有切實可行的步驟，確保資料使用者持有的個人資料不受未獲准許或意外地被查閱、處理、刪除、喪失或其他用途：

The Association should take all practicable steps to safeguard personal data from

unauthorized or accidental access, processing, erasure, loss or other uses by adopting the following measures:

- 查閱控制 Access control
  - 協會的內部政策規定查閱及處理個人資料受“需要知道”及“需要使用”的原則所規限。(例如當處理人力資源事務的職員調任到其他崗位時，其獲取人事檔案的權限應立即終止)。

    Personal data collected and retained should be disseminated to another party only if necessary. Access based on a “need to know” and “need to use” basis (e.g., when a staff who handles human resources, matters are transferred to another post, his/her right of access to personnel records should cease immediately).
  - 確保能查閱該資料的人的良好操守、審慎態度及辦事能力(例如要求新職員閱讀《保障個人資料私隱政策》、要求職員定期參加保障資料培訓、執行委員簽署保密聲明等)。

    Ensure the integrity, prudence and competence of authorized persons (e.g., requiring new staff to read the Code of Practice on Data Protection, requiring staff to participate in data protection refresher workshops periodically, signing of a confidentiality statement by Executive Committee Members, etc.).
  - 除特殊情況下(如在辦公室外進行的活動)，個人資料不可帶離辦公室。

    Personal data should not be taken away from the office, unless under special circumstances (e.g., events that take place outside the office).
  - 如聘請資料處理者（例如服務供應商)，必須採取合約規範方法或其他方式，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外的被查閱、處理、刪除、喪失或使用。

    If a Data Processor (e.g., service provider) is engaged, contractual or other means must be adopted to prevent unauthorized or accidental access, processing, erasure, loss or use.

- 資料儲存 Data storage
  - 應將個人資料存放在安全、適當的位置儲存（例如，可上鎖的文件櫃或管制區的房間)。包含個人資料的檔案不應留在桌面或任何未經授權人員可看到的區域。

    An appropriate physical location should be identified where the personal data can be safely stored (e.g., lockable filing cabinets or rooms with controlled access or which can be locked when unoccupied). Files containing personal data should not be left open on desks or in areas where they can be seen by

unauthorized persons.

- ■ 個人或敏感資料不應存儲在便攜式設備上，如外置記憶體、筆記本電腦或平板電腦。如果必須暫時將此類資料存儲在便攜式/移動設備上，所儲存的資料則應僅為必要資料並且具有密碼保護。此外，必須在完成所需工作後盡早刪除該資料。

  Personal or sensitive data should not be stored in portable devices, such as USB flash drives, notebooks or tables. In case such data has to be stored in portable/mobile devices temporarily, the data stored should be the minimum necessary and should be password-protected. Moreover, the data must be deleted as soon as the tasks for which it is required has been completed.

- 資料傳輸 Data transmission
  - ■ 確保個人資料的安全傳輸（例如包含個人資料的文 件應放進標密封的信封內，註明「私人密件」和「僅由接收資料者收閱」 的密封信封中並註明特定收件人）

    Adopt appropriate measures to ensure the secure transmission of personal data (e.g., documents containing personal data should be put in a sealed envelope marked “private and confidential” and to be opened by addressee only” with a specified addressee).
  - ■ 使用電腦系統中的共享雲端硬碟（如有）時，盡可能在安全和保密的環境中傳達個人資料。

    Make sure of shared drives in the computing system if available and, as far as possible, communicate personal information in a safe and restricted environment.
  - ■ 在傳輸電子郵件中採用加密軟件等保安措施，亦應仔細檢查電子郵件地址和附件以確保其正確無誤。

    Personal or sensitive data, when sent electronically, should be password-protected. Email addresses and attachments should be double-checked to ensure that they are correct.
  - ■ 在發送大量電子郵件時，應使用密件副本（BCC）或郵件合併功能以避免洩露收件人的電子郵件地址。

    When sending out a mass email, BCC or mail merge should be used to avoid disclosing the email addresses of recipients.
- 資料處置 Data disposal
  - ■ 個人資料需在特定的保留期限過後妥善處置，例如撕碎複印文件，磁盤和記憶棒格式化。

    Personal data should be disposed of properly after the specified retention period, e.g., hard copy documents should be shredded while disks and memory sticks should be formatted.

- 如在統計分析中可能識辨資訊當事人的身份，應予以匿名化處理。
  Information which can lead to the identification of the Data Subject in statistical analysis should be anonymized.

原則 5 - 透明度

DPP5 - Openness

協會將向所有持份者提供以下資訊：

The Association will make available the following information to all stakeholders:

- 在個人資料方面的政策及指引 Personal data policies and practices adopted；
- 持有的個人資料的種類 Types of personal data held；和 and
- 個人資料是為或將會為甚麼主要目的而使用 Purposes for which the personal data is used or to be used。

原則 6 - 查閱及改正

DPP6 - Data Access & Correction

- 資料當事人有權要求查閱他/她自己的個人資料，以及有權要求改正有關資料；

  A Data Subject must be given access to his/her own personal data and allowed to make corrections if it is inaccurate;
- 資料查閱要求是個人向資料使用者提出要求：

  A data access request is a request made by an individual to request the Data User:
  - 告知他/她有關資料使用者是否持有其個人資料 To inform him/her whether the Data User holds personal data of which the individual is the Data Subject；和 and
  - 如果資料使用者持有此類資料，向其提供該資料的副本 If the Data User holds such data, to supply him with a copy of such data；
- 資料當事人需使用個人資料私隱專員所規定的表格 2 提出查閱資料要求；

  Data Subjects shall submit Data Access Requests using Form OPS003 (Form 2) as prescribed by the Office of the Privacy Commissioner for Personal Data;
- 當協會收到資料查閱要求時，秘書處應該：

  When the Association receives a data access request, the Secretariat should:
  - 確定請求者的身份 Ascertain the identity of the requestor；和 and
  - 查閱體育總會是否持有相關個人資料 Assess whether the Association hold the relevant personal data；
- 協會如持有相關個人資料，需要在收到請求後 40 日內，依從資料當事人有關查閱資料的請求；

  If the Association holds the relevant personal data, a copy of the requested data should be supplied to the Data Subject with 40 calendar days after receiving the

request;

- 協會如並未有持有所請求的資料，亦需要在 40 日內以書面形式做出回覆；
  If the Association does not hold the requested data, the requestor should still be informed in writing within the 40-day time limit;
- 協會可以就依從查閱資料要求而收取合理的行政費用；
  The Association may impose an administrative fee for complying with a data access request which should not be excessive;
- 在以下情況，協會可拒絕依從查閱資料要求：
  The Association may refuse to comply with a data access request if:
  - 提出要求者沒有提供足夠的資料以識別請求者身分 It is not supplied with sufficient information to identify the requestor；
  - 遵從該項要求會導致資料使用者披露其他人的個人資料 It cannot comply with the request without disclosing the personal data of a third party；或 or
  - 在當其時，根據本條例或任何其他條例禁止遵從該要求 Where compliance with the request is for the time being prohibited under the Personal Data (Privacy) Ordinance or any other ordinance；
- 應保留紀錄備存過去四年的所有資料查閱要求，並將拒絕查閱資料要求記入記錄。
  Record should be kept to register all data access requests for the past four years, stating reasons if any of them are refused.

<u>行使拒絕要求 Opt-out Request</u>

資料當事人可隨時要求資料使用者停止使用其個人資料作直接促銷。資料當事人可透過口頭或書面方式傳達拒絕服務要求。

In direct marketing, a Data Subject may at any time require a Data User to cease using his/her personal data. Such "Opt-out" requests may be communicated verbally or in writing.

為有效依從資料當事人的拒絕服務要求，參與直接促銷的職員應建立一份「拒絕服務名單」並列出所有表示不希望收到進一步促銷資訊的人士。

To comply with a Data Subject's 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.

<u>處理資料外洩 Handling of Data Breach</u>

- 如果發生資料外洩，應首先向總幹事通報事故。
  In case of a data breach, the incident should be reported to the General Secretary in

the first instance.

- 應須迅速收集事故的所有相關資訊。
  Essential information related to the breach should be gathered.
- 在適當情況下通知以下各方：
  The following parties may also be notified as appropriate:
  - 有關執法部門 Law enforcement agencies；
  - 個人資料私隱專員公署 Office of the Privacy Commissioner for Personal Data；和 and
  - 資訊科技專家 IT experts。
- 應採取遏止措施來控制洩露事件（例如，停止可能與事故有關的系統功能或移除涉嫌造成或引致資料外洩的用戶的查閱權）。
  Measures should be adopted to contain the breach (e.g., cessation of a system function or access right).
- 評估事件可造成的損害。
  An assessment of the potential damage and harm caused by the breach should be made.
- 應考慮通知受影響的資料當事人和相關人士有關該次外洩事故。當資料當事人 無法立即被識別或存在公共利益時，可考慮通過協會網站或媒體進行公開通知。
  Consideration should be taken to notify affected Data Subjects and relevant parties of the breach. When Data Subjects are not immediately identifiable or where public interest exists, public notification through the Association's website or media may be considered.
- 應檢討資料外洩事故，向執行委員會報告全面的資料外洩事故紀錄。
  A thorough investigation into the breach should be carried out. The investigation results should be reported to the Executive Committee and kept in a detailed report.
- 應識別需要改進的地方，防止同類事故再次發生。
  Areas for improvement should be identified to prevent the breach from recurring.
- 應使用附件 4 中的「資料外洩事故通報表格」來整合與外洩事件相關的資訊，採取補救措施並進行事後檢討。
  The Data Breach Information Sheet should be used to consolidate information relating to the breach, take remedial actions and conduct post-incident review.

<u>檢討及修訂 Review and Revision</u>

本政策及有關措施的內容，將適時進行檢討及修訂。

The Association will review and, where necessary, revise this Policy and the related measures from time to time to ensure their effectiveness and compliance with prevailing legislation, regulatory requirements and best practices.

訂立日期 Effective Date：22/9/2026
修訂日期 Last Updated：-