



THE KENDO ASSOCIATION OF HONG KONG, CHINA

GUIDELINES AND PROCEDURES ON INFORMATION SECURITY

Objective: To ensure the security of computer systems and data, and to better manage the information technology resources and communication systems of the Kendo Association of Hong Kong, China Limited ("HKKA"), these guidelines and procedures are formulated to safeguard the use of computer files, emails, and any other means used to store, transmit and process information, consistent with article 70B 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. Discipline

- 1.1 The following activities shall not be conducted:
 - (a) accessing computers without authorisation;
 - (b) accessing a computer with criminal or dishonest intent;
 - (c) criminal damage, such as destroying webpages or spreading computer viruses;
 - (d) accessing network resources without authorisation;
 - (e) cracking, stealing or misappropriating other persons' accounts and passwords; and
 - (f) disclosing other persons' accounts and passwords without proper reason.
- 1.2 Accessing or downloading pornographic materials is strictly prohibited.
- 1.3 It is prohibited to produce, access, download or forward offensive, immoral, discriminatory or insulting data, or to make any vulgar remarks, suggestions or comments that may embarrass or humiliate members of the HKKA or any third party.
- 1.4 The HKKA's resources and working time are reserved for the operation of the HKKA. Using a computer for private or commercial purposes (such as accessing chat rooms, playing games or similar activities) during working hours is not allowed. Browsing non-business-related websites should be minimised to avoid unnecessary bandwidth congestion.
- 1.5 Spreading computer viruses or other interference or destruction programs on the internet or on other persons' computers is not allowed.
- 1.6 Use of peer-to-peer transmission software to share or download files is not recommended.
- 1.7 External storage media (e.g. USB drives) and files from unknown sources must not be used unless they have been checked and cleared of viruses and malicious code.
- 1.8 Do not download or execute any program or software from the internet unless approved by the Incident Coordinator referred to in section 5 below or another person designated by the Executive Committee for this purpose.

- 1.9 Do not upload any information relating to the HKKA to an external website without proper authorisation.

2. Security and Protection

- 2.1 Multi-factor authentication (MFA) shall be enabled on all HKKA email accounts, cloud storage, and other systems that support it, particularly where the account can access personal data or financial information. Where a system does not support MFA, an alternative compensating control (e.g. restricted access, additional monitoring) should be considered.
- 2.2 All desktops, laptops and other devices used to access HKKA systems should be protected by a strong, unique password or passphrase. The following are recommended:
- (a) a password or passphrase of at least 12 characters, combining upper case, lower case, numbers and a special character or symbol, or alternatively a longer passphrase of unrelated words that is easy for the user to remember but hard for others to guess;
 - (b) a password or passphrase must always be changed immediately upon any suspicion that it has been compromised; as an additional and optional safeguard, some users may also find it useful to change their password or passphrase periodically (for example, every three months);
 - (c) a changed password must not be the same as any of the previous three passwords used for that account;
 - (d) avoid passwords that are easy to guess (e.g. initials, birthdays) or common words (e.g. "password", "qwerty"); and
 - (e) avoid a series of consecutive letters or numbers on the keyboard, or repeated characters.

Multi-factor authentication under section 2.1 above remains the primary control and should be enabled wherever available.

- 2.3 Do not connect an HKKA device to an unreliable or unknown wireless network.
- 2.4 All staff should take proper care of their devices (desktops, laptops, mobile devices), particularly when travelling. Where a device is left unattended, the device owner should use a proper security tool (e.g. a laptop security lock) to keep it safe.
- 2.5 The HKKA shall ensure its information systems are protected from threats by installing anti-virus and firewall systems. If a computer virus infection is suspected, the user must stop using the computer immediately and report the issue to the Incident Coordinator referred to in section 5 below, in accordance with the HKKA Incident Response Procedure.
- 2.6 The HKKA shall conduct regular security risk assessments and internal compliance audits, including reviews of information system updates, vulnerability repairs, patch installation, authority management and security configuration, to identify potential security weaknesses and seek resolutions.
- 2.7 Do not place drinks or small stationery items near computer equipment, so as to minimise the risk of damaging the device.
- 2.8 The practice of switching off computers before leaving the workplace should be adopted.
- 2.9 Do not disassemble or modify any office device.

- 2.10 A report should promptly be made if a device or data is lost, stolen or damaged, in accordance with the HKKA Incident Response Procedure.
- 2.11 Users are not allowed to use personal or private devices for HKKA business communication, save where the Executive Committee has approved a bring-your-own-device arrangement subject to appropriate safeguards.
- 2.12 Be aware of phishing emails. Do not access suspicious links or open suspicious attachments. Do not forward or reply to suspicious emails; delete them promptly and report them to the Incident Coordinator referred to in section 5 below.
- 2.13 A communication account shall only be available to the authorised person, and account sharing is not allowed.

3. Backup and Archive

- 3.1 Users shall perform regular backups of work-related data and information.
- 3.2 Confidential or sensitive data should, where practicable, be physically or logically isolated from external networks.
- 3.3 The HKKA shall enable encryption options (where available) when backing up sensitive or confidential information.

4. Copyright

Only licensed software may be installed on HKKA devices, in compliance with the applicable licence agreement.

5. Emergency and Incident Response

Where a security incident occurs or is suspected (including suspected unauthorised access, malware, or loss of a device or data), the matter shall be handled in accordance with the HKKA Incident Response Procedure, which sets out the escalation, containment and reporting steps to be followed. The HKKA shall publish the name, post or designation, and contact telephone number of the person responsible for coordinating the response to a security incident (the Incident Coordinator), to facilitate the seeking of immediate assistance.

Any personal data collected, used or retained in connection with this document shall be handled in accordance with the HKKA Guidelines and Procedures on Personal Data Privacy Protection. Where personal data is collected directly from an individual using a form referred to in this document, the individual shall be provided with a Personal Information Collection Statement consistent with Appendix II to the HKKA Guidelines and Procedures on Personal Data Privacy Protection. In particular, where a security incident involves personal data, it shall additionally be handled under the data breach provisions of the HKKA Guidelines and Procedures on Personal Data Privacy Protection.

6. Training

The HKKA should ensure that all staff are made aware of the requirements in this document and shall arrange briefings or training to enhance awareness of information security, including how to recognise phishing attempts and how to use multi-factor authentication.

7. 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