Document Title	SCoT IT Usage & Management Policy		
Published	Jan 2021	**Version**	1.1
Approved	Jan 2021		
Author	Chair Reviewed: Membership Director		
Review	Due: Jan 2023 Reviewed:		

SCOTTISH COUNCIL OF TAEKWONDO

IT USAGE & MANAGEMENT POLICY

1. Reasons for having this policy

All SCoT's IT facilities software and corporate information resources remain the property of SCoT and not of particular individuals, teams or departments (Note1). By following this policy we'll help ensure the most appropriate and correct IT assets are used and kept secure:

- legally;
- securely;
- without undermining SCoT;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so they remain available.

The policy relates to all Information Technology facilities and services provided by SCoT. All staff and volunteers are expected to adhere to it.

2. Disciplinary Measures

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include the offender being denied access to computing facilities.

2.1 Copyright:
Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

2.2 Security:

- Don't attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents.
- If you don't have access to information resources you feel you need, contact the SCoT Board.
- Don't disclose personal system passwords or other security details to any other staff, volunteers or external agents and don't use anyone else's login; this compromises the security of SCoT.
- If someone else gets to know your password, ensure you change it or get an appropriate person in the organization to help you (Note2).
- If you leave your PC unattended without logging off, you are responsible for any misuse of it while you're away from keyboard or “AFK”.
- ALWAYS check external media for viruses, even if you think they are clean – ScoT Directors, staff/ consultants or anyone are expected to utilize up to date AntiVirus and Securoty software
- Computer viruses are capable of destroying SCoT's information resources. It is better to be safe than sorry.

2.3 Information about people: If you're recording or obtaining information about individuals make sure you are not breaking Data Protection legislation and are fully complying with the SCoT policies on Data Protection and Information Security

2.4 You are a representative of SCoT when you're on the Internet using email or representing the organization in any Directorial or Staff capacity:

- Make sure your actions are in the interest (and spirit) of SCoT and don't leave SCoT open to legal action (e.g. libel).

- Avoid trading insults with other people using the Internet with whom you disagree.

- Obscenities/Pornography: Don't write it, publish it, look for it, bookmark it, access it or download it.

2.5 'Electronic monitoring': Any information available within IT facilities must not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, Internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are:

- In the case of a specific allegation of misconduct, when the Management Team can authorise accessing of such information when investigating the allegation.

- When ~~the~~ an authorized individual is providing IT Support ~~section~~ and cannot avoid accessing such information whilst fixing a problem.

In such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary. In the former case their access to IT facilities may be disabled pending investigation.

3. Email Policy

3.1 When to use email:

- Use it in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. Think and check messages before sending (just as you would a letter or paper memo).

- Use the phone (including voicemail if no reply) for urgent messages (email is a good backup in such instances).

3.2 Use of Distribution Lists:

- Only send Email to those it is meant for; don't broadcast (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer performance and wastes disc space.

- Use the standard aliases (Note 3) for work related communication only.

- If you wish to broadcast other non work related information or requests (e.g. information or opinions on political matters outside the scope of SCoT's campaigning, social matters, personal requests for information etc.) it is better to use a Webmail account (Note4) or a personal email account at home; don't use the standard (work) aliases.

- Keep SCoT's internal email aliases internal. If you are sending an email both to a SCoT alias and outside of SCoT, use the alias as a blind carbon copy (i.e. the bcc address option) so that the external recipient does not see the internal alias.

- Don't broadcast emails with attachments to large groups of people. Either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

3.3 General points on email use:

- When publishing or transmitting information externally be aware that you are representing SCoT and could be seen as speaking on SCoT's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager or The Board of SCoT.

- Check your in-box at regular intervals during the working day (staff only). Keep your in-box fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

- Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.

- Use prefixes in the subject box whenever appropriate (Note5).

- Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions / decisions of a colleague).

- Don't forward emails warning about viruses (they are invariably hoaxes themselves)

3.4 Email etiquette :

- Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are also copying another group of people.

- Make your subject headers clear and relevant to your reader(s) eg Don't use subject headers like "stuff". Don't send a subject header of, say "accounts" to the accountant

- Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.

- Using asterisks at each end of a word (eg *now*) is common practice for highlighting text.

- Capitals (eg NOW) can also be used to emphasise words, but should be used sparingly as it commonly perceived as 'shouting'.

- Don't open email unless you have a reasonably good expectation of what it contains, eg Do open report.doc from an Internet colleague you know. Don't open explore.zip sent from an address you've never heard of, however tempting. This is one of the most effective means of protecting SCoT against email virus attacks.

- Keep email signatures short. Your name, title, phone/fax and web site address may constitute a typical signature.

- Understand how forwarding an email works. If you forward mail, it appears (to the reader) to come from the originator (like passing on a sealed envelope). If you forward mail *and edit it* in the process, it appears to come from you - with the originator's details usually embedded in the message. This is to show that the original mail is no longer intact (like passing on an opened envelope).

4. Miscellaneous

4.1 Hardware and Software: All purchases should be approved by your line manager (for employees) or by an appropriate budget holder on the Board of Directors

4.2 Installing Software: Get permission from your line manager or SCoT Board before you install any software (including public domain software - see Note6) on equipment owned and/or operated by SCoT.

4.3 Data transfer and storage on the network:

- Keep master copies of important data on SCoT's cloud storage and not solely on your PC's local C: drive or removable drives or media. Otherwise it will not be backed up and is therefore at risk.

- Ask for advice from your line manager or SCoT Board-if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill.

- Be considerate about storing personal (non- SCoT) files on SCoT's network. (Note7). The general rule is that no personal files should be kept or maintained on any SCoT owned devices nor on SCoT's shared folders / cloud storage.

- Don't copy files which are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disc space unnecessarily.

4.4 Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, playing computer games and browsing the Internet) is permitted so long as such use does not:

- Incur specific expenditure for SCoT
- Impact on your performance of your role (this is a matter between each member of staff and their line manager).
- Break the law
- Bring SCoT into disrepute.
- Is undertaken during your normal hours of work

4.5 Care of equipment:

- Members of SCoT staff, Board and volunteers who have access to or have in their possession IT equipment and devices owned by SCoT are expected to treat such equipment and devised in a reasonable and professional manner.

4.6 Passwords & Protection

- SCoT ask that you change your password every 30 days if you are accessing the SCoT SharePoint cloud server. There are only limited logins available to SharePoint and it is critical to keep it secure.
- Password advice is to use 4 unconnected random words as there is less chance of Malware being able to crack codes – example is “CatSkipTrousersBus” – as silly as it looks and sounds, it is more secure than most passwords
- Users with access to sharepoint will have an automatic prompt ever 30 days to change password and also be required to use Microsoft Authenicator for two-step authorization.
- For staff or critical role, SCoT will reimburse expense of procurement of AntiVirus Security software such as Kaspersky (recommended) Norton, Eset or McAfee.

4.7 Microsoft SharePoint & Office365

- SCoT has begun introduction and roll-out of Microsoft Office 365 and SharePoint within the organization. Currently, there are 2 “Basic” Licences purchased with potential for more at a later date.
- Current users are the Chair and the Membership Director. Those roles have the most IT and document-reliant workload and all files were recently transferred over to the secure SharePoint document library.
- Only users with username and password and who pass the 2-factor authentication are allowed access. It is extremely secure and also allows for “one file – used many times” to prevent duplication of files and workload

NOTES

(1) In-house software: This is software written by staff or volunteers using SCoT's equipment. It is SCoT's property and must not be used for any external purpose. Software developers (and students) employed at SCoT are permitted to take a small "portfolio" of such in-house software source code/ executables, which they may have developed, for use in subsequent work, subject to agreement with the appropriate line manager and/or Board member.
(2) Personal passwords: Follow Password Policy
(3) Email aliases are pre-defined 'shortcuts' for distributing internal email to specific groups of people.
(4) Webmail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser, eg home or cybercafe.
(5) Subject box prefixes: These are ''U:' for Urgent', 'FYI' for your information and 'AC:' requires action. If the email is a very brief message confined solely to the subject line, it should in addition be prefixed with '**' to indicate "just read this line".
(6) Public domain software or Freeware: This is software that is available free of charge, usually by

downloading from the Internet.

(7) Personal Data: As a guideline, keep your personal data down to 10MB. Ten emails require 0.15MB on average (depends a lot on whether they have attachments). A 10-page word processed document requires about 0.1MB.