

INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

UPDATED: OCTOBER 2023



Scottish
Volleyball

Information and Communication Systems Policy

Introduction

Scottish Volleyball Association (SVA) is heavily dependent on computer systems and the information that they generate to achieve its aims and objectives. ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form. The SVA ICT systems are intended to promote effective communication and working practices. This policy outlines the standards employees must observe when using these systems, when we will monitor their use, and the action we will take if any staff member breaches these standards.

Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Equipment Security and Passwords

Employees are responsible for the security of the equipment allocated to or used by them, and the employee must not allow it to be used by anyone other than in accordance with this policy. The employee should use passwords on all IT equipment, particularly items that they take out of the office.

The employee should keep passwords confidential and change them regularly.

Employees must only log on to the SVA systems using their own username and password. The employee must not use another person's username and password or allow anyone else to log on using their username and password.

If an employee is away from their desk they should log out or lock the computer and must log out and shut down their computer at the end of each working day. An inactivity time-out should be set-up on all computers/devices and this should be set to an inactive period after 5 minutes.

Systems and Data Security

Employees should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties). Employees must not download or install software from external sources without authorisation from the CEO or Office Manager. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

Employees must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the CEO or Office Manager.

We monitor all e-mails passing through our system for viruses. Employees should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

Employees should inform the Office Manager immediately if they suspect their computer may have a virus.

E-mail

E-mail is a primary communication tool, both internally and also with external third parties. All e-mail data stored on the SVA servers is SVA property and the SVA can deal with such data in whatever manner it may decide.

Employees must adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

Employees must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

Employees should not:

- ❧ send or forward private e-mails at work which they would not want a third party to read.
- ❧ send or forward chain mail, junk mail, cartoons, jokes or gossip.
- ❧ contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them;
- ❧ send messages from another person's e-mail address (unless authorised) or under an assumed name;
- ❧ send or forward political and commercial content;
- ❧ send or forward confidential information without applying additional protection (e.g. password protected document);
- ❧ use the SVA e-mail system to infringe the copyright or other intellectual property rights of third parties; or
- ❧ use their own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for them.

Employees must notify the CEO or Office Manager immediately if you receive an e-mail that is inappropriate or offensive.

If employees have access to their emails on mobile phones or other any other device then the appropriate secure measures must be put in place – all devices must be password protected.

Use of shared email inboxes

As Scottish Volleyball grows as an organisation, the need for shared mailboxes becomes imperative for good communication both within departments and interdepartmentally. To ensure consistency across the organisation, employees should comply by the following rules:

- 🌀 All communication related to your specific job role should be done through the shared inbox associated with it. For example, if you are dealing with a finance issue, then emails should be sent from finance@scottishvolleyball.org.
- 🌀 When sending emails, signatures must be used to ensure that those who you are communicating with are aware of who they are speaking to. Signatures should be regularly checked to confirm that they are up to date.
- 🌀 A personal email is defined as your Scottish Volleyball email unique to you which will, as much as is possible, be consistent with the rest of the SV staff. Your license for use of Office 365 products is through this email.

A private email is defined as your own email out of Scottish Volleyball such as a gmail or btinternet account.
- 🌀 For any correspondence that does not directly relate to your job role or is private in any way, then use of a personal email is acceptable. This can also be used for meeting bookings and annual leave or TOIL requests.
- 🌀 For any correspondence that should not be seen by any other staff or persons associated with Scottish Volleyball, then use of a private email is recommended. This could be for raising welfare or disciplinary complaints for example.

Using the internet

Internet access is provided primarily for business purposes.

Employees should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

We may block or restrict access to some websites at our discretion.

Social Media

Social Media refers to interaction among people in which they create, share and/or exchange information and ideas in virtual communities and networks. When someone clearly identifies their association with the SVA and/or discusses their work, they are expected to behave appropriately when on the internet, and in ways that are consistent with SVA values and operational policies.

Personal use of our systems

We permit the incidental use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use must meet the following conditions:

- 🌀 it must be minimal and take place exclusively outside of normal working hours (that is, during lunch breaks, and before or after work);
- 🌀 personal e-mails should be labelled "personal" in the subject header;
- 🌀 it must not affect the employees work or interfere with the business;
- 🌀 it must not commit us to any marginal costs; and
- 🌀 it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Procedure.

Monitoring

The SVA systems enable us to monitor telephone e-mail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, employees use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- 🌀 to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
- 🌀 to find lost messages or to retrieve messages lost due to computer failure;
- 🌀 to assist in the investigation of alleged wrongdoing; or
- 🌀 to comply with any legal obligation.

HARDWARE PURCHASE AND REPLACEMENT

The SVA will make every effort to replace equipment that falls below the standards required to carry out the associated work for which the equipment is required.

ICT SUPPORT

Technical support is currently contracted through Mear Technology. Any ICT issues which cannot be solved internally should be referred to MearTechnology, via Tel: 01506 66 86 13 or email: helpdesk@meartechnology.co.uk

LOSS OR DAMAGE OF INFORMATION

All SVA files are stored on the main server and daily back-ups are undertaken in the event of hardware failure. Any loss or damage should be reported to the Office Manager for action.

ICT TRAINING

New employees will be expected to have knowledge of ICT as a basic condition of employment. Further employee training needs will be identified during appraisal meetings with employees.

DISCLAIMERS

In order to reduce the risk of prosecution for transmitting incorrect or inappropriate information, all SVA e-mails are sent with a disclaimer attached. The disclaimer reads: "The information contained in this message is confidential to the recipient. The dissemination, distribution, copying or disclosure of this message or its contents is prohibited unless authorised by the sender. If you receive this message in error, please immediately notify the sender and delete the message from your system. Please note that neither Scottish Volleyball Association, nor the sender accepts any responsibility for viruses and it is your responsibility to scan this message and any attachments. No contractual commitment may be entered into by Scottish Volleyball Association by virtue of e-mail alone."

However, employees are reminded that the same laws apply to e-mail as any other written document and accordingly employees must avoid sending inaccurate or defamatory statements or inappropriate material under the SVA banner, irrespective of the status of the intended recipient or their relationship to the sender.

Prohibited use of our systems

Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

- pornographic material (that is, writing, picture's, films and video clips of a sexually explicit or arousing nature);

- Ⓢ offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
- Ⓢ a false and defamatory statement about any person or organisation;
- Ⓢ material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Preventing and Dealing with Harassment and Bullying Policy);
- Ⓢ confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);
- Ⓢ unauthorised software;
- Ⓢ any other statement which is likely to create any criminal or civil liability (for you or us); or
- Ⓢ music or video files or other material in breach of copyright.

Leaving Employment

Upon leaving the SVA, employees must return their SVA handset, SIM Card, battery and charger to the Officer Manager. Employees using their own phones for business use will be required to delete emails before their employment ends. Evidence of such action will be required by the CEO as any breach of confidential/data protection breach by the employee may result in prosecution.

The Office Manager will inform the IT Contractors that a staff member is leaving the association 3 days prior to their last day asking them to ensure that all access to the SVA systems are immediately revoked after a certain time on the leaving date. If confirmation of this action is not received by the Office Manager within 24 hours of the leaving date a follow up email/call must be made to ensure this action is carried out. Once confirmation is received from the IT contractors this must be recorded and filed.

For more information or questions you may have regarding this policy, please contact the Office Manager in the first instance.