Scottish Disability Sport

INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) POLICY

Reviewed by Board – December 2022

Introduction

Scottish Disability Sport (SDS) is heavily dependent on computer systems to achieve its aims and objectives. ICT covers any product that will process, store, retrieve, manipulate, transmit or receive information electronically in a digital form. For example, personal computers, laptop computers, digital cameras, emails, smartphones, tablets, etc.

This policy provides guidance on what individual responsibilities are and the processes adopted by SDS. Companies who do not comply with the legal guidelines set down for computer use leave themselves vulnerable to an unlimited fine or imprisonment. It is vital that we all work together to ensure compliance.

Part of your ICT responsibility is to ensure that you show good working practices when using the equipment and do not compromise SDS either ethically or legally. The e-mail system is first and foremost a tool to be used in the context of work. Employees should be aware that a breach of the rules on the ICT Policy could be viewed as gross misconduct and will entitle SDS to take disciplinary action against the relevant member of staff in accordance with the disciplinary procedures.

This policy applies to all persons working for SDS or on behalf of the Association in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners. This policy does not form part of any employee's contract of employment and we may amend it at any time.

SDS Services

In SDS terms, ICT is categorised into two broad categories of product:

1. The traditional computer-based technologies, e.g. things you can typically do on a personal computer, laptop or tablet;
2. Digital communication technologies which allow people and companies to communicate and share information digitally.

Category one includes the following non-exhaustive list of services:

- Software applications, primarily Microsoft Office but including approved database, design and accounting software. Outcomes include the preparation and distribution of agendas, minutes, letters, reports, presentations, company accounts and emails; facilitation of online learning; registration for and records of events and training courses.

Category two includes the following non-exhaustive list of services:

- Website administration;
- Production of electronic surveys;
- Digital video/voice communications and online meetings;
- Online document storage, e.g. Dropbox, OneDrive, Google Docs;
- Online document transfer, e.g. WeTransfer, What's App;
- Social media communication; and
- Online accounting and HR services.

Managing ICT

The main ICT hub for SDS is the Edinburgh Office which is organised by the Senior Administrator with Regional staff accessing the hub from external sites. The ICT systems are operated by the employees and occasionally ICT equipment is accessed by volunteers when operating on behalf of SDS.

Internet

The internet is used for business purposes and also for incidental personal purposes. This does not, however, include use which involves substantial expenditures of time not connected with business purposes, use for profit, use to access pornography or use which would otherwise violate SDS policy.

Employees must ensure that they:

- Do not engage in activities on the internet which might bring SDS into disrepute.
- Do act in a transparent manner when altering online sources of information.
- Do not use the internet in any way to attack or abuse colleagues.
- Do not post derogatory or offensive comments on the internet.

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 SDS and/or discusses their work, they are expected to behave appropriately and in ways that are consistent with SDS's values and operational policies. Staff will follow SDS Social Media Guidelines when using this medium of communication.

Email

Email is a primary communication tool, both internally and externally. All email data is the property of SDS and SDS can deal with such data in whatever manner it may decide.

Standards to uphold when using email

- Email should be considered as a formal means of communication and should be treated similarly to written or verbal communication. Remember to be respectful and polite.
- Do not use email for political or commercial reasons – it should generally be used for business purposes only.
- It is acceptable, within reason, to also use email for personal purposes. Time sent using email for personal purposes should, however, be kept to a reasonable minimum during business hours and should not involve substantial expenditures of time, use for profit or use which would otherwise violate SDS policy.
- Files should only be sent by email when there is no alternative in order to avoid duplication of shared documents.
- Email is not secure – do not use it for confidential information without applying additional protection (e.g. password protect document).
- Do not use SDS's email system to infringe the copyright or other intellectual property rights of third parties.
- Do notify your line manager immediately if you receive email that is inappropriate or offensive.
- Employees should be aware of the types of email likely to be a threat to cyber security.

Monitoring

SDS may engage in the monitoring of electronic mail messages or other electronic files created by staff for valid business purposes, including employee supervision. SDS may also monitor any email messages or other electronic files created by employees for personal purposes.

Hardware Purchase and Replacement

All SDS hardware will be written off after between three and five years. An audit of ICT needs will be conducted each financial year to determine the company's needs and determine the ICT requirements to meet said needs. SDS 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. Hardware will be disposed of securely by SDS's ICT support contractors.

Software

SDS will not use illegal software. Software disposal will be undertaken by SDS's ICT support contractors. Staff are discouraged from deleting software programmes themselves. You should notify your line manager who will arrange the proper deletion of software. Any abuse of ICT equipment or systems by employees will result in disciplinary action being taken.

ICT Support

Technical support is currently contracted through Mear Technology and the JustGo database support is included in their contract and annual payment. Existing ICT support agreements will be evaluated annually to assess future technical support requirements and ensure cost-efficient services.

Any ICT issues which cannot be solved internally should be referred to Mear Technology by logging with the helpdesk using login details supplied to each individual. Alternatively phone Mear Technology on 01506 668 613.

Loss or Damage of Information

All SDS files are stored on the cloud. Any loss or damage should be reported to the Senior Administrator for action.

Budgeting for ICT

A budget will be allocated for the preparation of the annual audit with all other expenditure being dealt with on a project to project basis. Any major purchases will only go ahead when a budget has been identified and approved. In addition to purchasing requirements for that year, a minimum amount will be allocated annually to build a fund to replace SDS hardware on a three to five year cycle.

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.

ICT Risk Assessment

An annual risk assessment of ICT will take place which covers:

- The nature of information;
- The management of information;
- The UK Data Protection Act 2018 and UK GDPR;
- Loss or damage of information;
- Physical theft;
- Unauthorised access to information; and
- User password protection.

Passwords

Employees are provided with an individual, confidential password or PIN, which they are required to input at the start of each session. SDS's ICT support contractors will ensure that all staff follow the password protection protocol:

- Employees will be prompted to change their password every 90 days.
- All passwords must contain a minimum of 8 characters.

Colleagues' passwords should never be used to gain entry to their computer. Employees should also be aware that they are responsible for the security of their own ICT equipment and should not allow any unauthorised person to use it. If there is any suspicion that password confidentiality has been breached, the employee must contact the Senior Administrator.

Disclaimers

In order to reduce the risk of prosecution for transmitting incorrect or inappropriate information, all SDS emails are sent with a disclaimer attached. The disclaimer states: "This document is confidential and intended for the use of the individual(s) to whom it is addressed. If you are not the intended recipient, please inform the sender immediately and be advised that any unauthorised use of this document is strictly prohibited."

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

Copyright Laws

Much of what appears on the internet by copyright, including photographs. The Copyright, Designs and Patents Act 1988 states that only the owner of the copyright is allowed to copy the information and copying without permission, including electronic copying, is prohibited. Employees should be aware that the copyright laws apply not only to documents but also to software and are strongly encouraged to contact the Senior Administrator for clarification.

Security

Keep equipment and data safe.

- Computer equipment and data should only be used for authorised purposes.
- Files, devices and software should be checked for viruses prior to installation.
- Dispose of confidential waste securely.

Portable computer equipment is a valuable and vulnerable commodity. Common sense should be applied at all times – for example, do not leave a laptop unattended, or visible in a car.

Home working is now commonplace across SDS and all staff should make every effort to ensure that portable computer equipment is operated and stored, safely and securely within the home environment.

Staff travelling out with the UK should inform the Senior Administrator as it may be necessary to increase SDS's insurance protection.

Health & Safety

Office furniture is to be ergonomically suitable and fit for purpose. The needs of staff will be checked on an annual basis. Employees are to be made aware of issues affecting repetitive strain injury sometimes caused by bad posture.