



**Scottish Association of
Local Sports Councils**

Information Communication Technology (ICT) Strategy



CONTENTS

Section 1: Introduction

SALSC Services

Section 2: The SALSC ICT Organisation

Hardware Purchase and Replacement

Software Policy

ICT Support

Loss or Damage of Information

Budgeting for ICT

ICT Training

ICT Risk Assessment

Health and Safety

Appendices: Appendix A –ICT Inventory

Appendix B –Email & Internet Security Policy

Appendix C – Recommendations for 2010



SECTION 1: INTRODUCTION

1.1 An ICT Strategy gives a planned and strategic approach to possibly the most important contributory factor to any modern organisations success. This strategy also creates a datum against which true progress can be monitored. However it is vitally important that ICT serves the needs of the organisation rather than becoming an end in itself.

1.2 A good way to think about ICT is to consider all the uses of digital technology that already exist to help individuals, businesses and organisations use information.

1.3 ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form. For example, personal computers, digital camera, email. So ICT is concerned with the storage, retrieval, manipulation, transmission or receipt of digital data. Importantly, it is also concerned with the way these different uses can work with each other.

SALSC Services

1.4 In SALSC terms, ICT is categorised into two broad types of product: -

1.4.1 The traditional computer-based technologies e.g. things you can typically do on a personal computer (PC)

1.4.2 The more recent and fast-growing range of digital communication technologies which allow people and organisations to communicate and share information digitally

1.5 Category one includes the following services:

1.5.1 Word processing delivered using Microsoft Word - Outcomes include the preparation of meeting agendas, minutes, letters and reports.

1.5.2 Spreadsheets delivered using Microsoft Excel - Database delivered using Microsoft Access and Word.

1.5.3 Presentations delivered using Microsoft Power Point - Outcomes include presentations to partners and members.

1.5.4 Emails communicated with Microsoft Outlook – Outcomes include the sending of electronic communications and scheduling of meetings.

1.5.5 Document Management using Adobe Acrobat Professional - Outcomes include document security.

1.5.6 Accounting delivered using Sage Financial Accounts - Outcomes include Budget, Profit & Loss, Prior Year and VAT Reports.

1.6 Category two includes the following services:

1.6.1 E-mail Administration

1.6.2 Website Administration

1.6.3 Production of Electronic Newsletters

1.6.4 Production of Electronic Surveys

1.6.5 Digital voice communications and online meetings



SECTION 2: THE SALSC ICT ORGANISATION

2.1 The main ICT hub for SALSC is organised by the Administrator and Policy Director. The ICT systems are operated by the staff with assistance from various volunteers. All PCs are linked by the internet.

(Refer to Appendix A)

Hardware Purchase and Replacement

2.2 All SALSC hardware will be written off over a period of three years. An audit of ICT needs will be conducted each financial year to determine the organisations needs and determine the PC specification required to meet said needs. SALSC will make every effort to replace PCs that fall below the standards with all new PCs using the new specification.

(Refer to Appendix A for a list of all SALSC hardware)

Software Policy

2.3 SALSC will not use illegal copies of software. Where functions are common, software will be standard across all office PCs. Any abuse of ICT equipment or systems by staff will result in disciplinary action being taken.

(Refer to Appendix A for a list of software)

ICT Support

2.4 Technical support for phones, email, PCs and internet is current supplied by Nanotech Scotland. All incoming and outgoing emails are scanned for viruses using a regular updating system currently supplied by Nanotech Scotland. Incoming emails are also checked for spam using a regular updating filter currently supplied by Nanotech Scotland. Research will be conducted every 3 years to ensure SALSC is receiving a competitively priced and appropriate service for its needs.

Loss or Damage of Information

2.5 All SALSC data files are stored on an External Hard Drive. A weekly recovery system is in place with all files backed up on a Friday afternoon.

Budgeting for ICT

2.6 A budget will be allocated for the preparation of the yearly 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 allocated. In addition to purchasing requirements for that year, a minimum amount (to be agreed) will be allocated annually to build a fund to replace SALSC hardware on a three year cycle.

ICT Training

2.7 New recruits will be expected to have knowledge of ICT as a basic condition of employment. Further staff training needs will be identified during the annual staff appraisal interviews.



ICT Risk Assessment

2.8 A yearly risk assessment of ICT will take place which covers:

- a) The nature of information
- b) The management of information
- c) Data Protection Act
- d) Loss or damage of information
- e) Physical theft
- f) Unauthorised access to information
- g) User password protection

Health & Safety

2.9 All SALSC staff will have access to a yearly eye test to determine if any eye strain has occurred. Office furniture is to be ergonomically suitable and fit for purpose. Staff are to be made aware of issues affecting repetitive strain injury sometimes caused by bad posture.



APPENDIX A

ICT INVENTORY

SECTION 1: SALSC HARDWARE & SOFTWARE

1.1 Laptop 01 (Administrator & Policy Director)

1.1.1 Hardware

None

1.1.2 Software

None.

1.1.3 Purchased on

N/A

1.2 General Software

1.2.1 Online Newsletter

Monthly Subscription to Mailing Manager
Purchased on 03/06/2009

1.2.2 Online Surveys

Annual subscription to Survey Monkey
Purchased on 27/04/09

SECTION 2: GENERAL OFFICE EQUIPMENT

2.1 Printer/Scanner/Photocopier/Fax Machine

Brother Fax 1360

Purchased on 2 March 2006



APPENDIX B: EMAIL & INTERNET SECURITY

Policy Statement

As an employer, the Scottish Association of Local Sports Councils (hereafter referred to as SALSC) expects that all its computer facilities be used in a professional and appropriate manner. Although SALSC is legally liable for employees' activities when using e-mail or the Internet at work, it is the responsibility of each employee to ensure that the technology provided for their use is used for proper work purposes and in a manner that does not compromise the organisation or its employees in any way. The following procedures and information are intended to advise employees of the types of e-mail and Internet use which SALSC considers appropriate and the possible consequences for employees using e-mail or the Internet in a way considered unacceptable. Accordingly, this policy document should be read in conjunction with SALSC's Disciplinary policy.

Benefits of E-mail and the Internet

Although e-mail communication has the same speed and apparent informality as using the telephone, it also has the permanence of written communications and as such must be controlled to ensure that it meets the same standards as other SALSC documents.

The advantages of e-mail include:

- It is a fast and inexpensive way of delivering messages and documents long and short distances
- Information can be shared quickly and consistently between any number of people
- It removes the excessive need to print and distribute information

The disadvantages of e-mail include:

- If it is used inappropriately, employees may suffer from "information overload", with vital information being lost amid excessive irrelevant messages
- It can stifle face to face communication or be used to abdicate the responsibility of communicating messages that should be done in person

The advantages of the Internet include:

- Access to large amounts of information from a wide variety of sources
- Information which is often more up-to-date than that found in traditional sources like libraries
- Speed of access to information

The disadvantages of the Internet include:

- Misuse which puts the organisation at technical and/or commercial risk
- The information posted on the Internet is unchecked and may be inaccurate
- Complex copyright issues

Internet & Email Access

All permanent employees of SALSC have access to e-mail and the Internet, either on their own desktop PC or at a terminal designated for general use. It is expected that during working hours that access to e-mail and the Internet be used for work-related purposes. Taking a realistic attitude, the SALSC Management Board accept that there may be occasions when individuals respond to personal e-mails or



make arrangements through e-mail during working hours. However, this must not be excessive and usage will be monitored. These privileges may be removed or amended at any time at the discretion of SALSC.

Employees are permitted to use e-mail for reasonable personal purposes. Employees must remember if they are sending personal e-mails from work that the SALSC disclaimer is displayed on every external e-mail and therefore personal e-mails are being sent under the SALSC banner.

Employees may also use the Internet for reasonable personal purposes. However, employees using the Internet for personal use must ensure that they are not using their access for illegal activities (e.g. computer hacking, attempting to disable or compromise security of information) or accessing inappropriate sites (e.g. pornography, betting/gambling sites, "hate" sites). Such use will result in a Disciplinary Investigation being carried out which may result in a formal Disciplinary Hearing being convened. This investigation may, in turn, lead to formal disciplinary action or dismissal.

Passwords

Employees are provided with an individual, confidential password, which they may be required to input at the start of each session. The Chairman must be informed of all passwords to ensure ICT services can continue in the situation of a member of staff leaving. Employees must not disclose their passwords to anyone else other than the Chairman. If there is any suspicion that password confidentiality has been breached, the employee must contact the Chairman as soon as possible to inform him/her and arrange a new password. Employees should also be aware that they are responsible for the security of their own terminal and should not allow any unauthorised person to use it.

Confidentiality

E-mail tends to be used in a more informal way than many other forms of communication. Employees should ensure that this informality does not lead to a lack of standards or a breach of confidentiality. As a rule, employees should not transmit anything by e-mail that they are not comfortable writing in a letter or memorandum. It should never be assumed that e-mails are completely private and confidential, even if marked as such. Matters of a sensitive or personal nature should not be transmitted by e-mail unless totally unavoidable. Employees should note that electronic messages are admissible as evidence in legal proceedings and have also been successfully used in libel cases.

Internet messages should also be treated as non-confidential. Anything sent via the Internet passes through a number of different computer systems, each with different levels of security. The confidentiality of messages may be compromised at any stage unless messages are encrypted. Postings placed on the Internet contain SALSC's address and for this reason, it is imperative that any posted information reflects the organisation's standards and policies. Employees are advised that under no circumstances should information of a confidential or sensitive nature be placed on the Internet. Employees should be aware that information posted or viewed on the Internet may constitute published material and therefore reproduction of such information may be done only with permission of the copyright holder.

Disclaimers



In order to reduce the risk of prosecution for transmitting incorrect or inappropriate information, all SALSC e-mails are sent with a disclaimer attached. The disclaimer states: “This document is confidential and intended solely 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 e-mail as any other written document and accordingly employees must avoid sending inaccurate or defamatory statements or inappropriate material under the SALSC banner, irrespective of the status of the intended recipient or their relationship to the sender.

Viruses

Viruses pose a serious threat to SALSC’s entire network, systems and property, with the greatest risk lying in downloaded programs and executable files. All software for SALSC use must be obtained from controlled legal sources **and authorised by the Management Board**. Employees should note that the spreading of viruses is subject to prosecution under The Computer Misuse Act 1990.

Copyright Laws

Much of what appears on the Internet is, or claims to be, protected by copyright. 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 Management Board for clarification.**

Content

E-mail is commonly used as a quick and informal way of contacting someone. However, because the communication is not face to face and there is no indication of tone/irony/body language etc, it carries the risk that the recipient will be offended, albeit unintentionally.

SALSC employees must therefore not send offensive, demeaning or disruptive messages. This includes, but is not limited to, messages inconsistent with SALSC’s Equal Opportunities and Anti-Bullying and Harassment policies. Employees should not place on the system any message, which could be regarded as potentially offensive. Abusive e-mails are sufficiently common to be given a name – flames – and SALSC employees must not send or respond in kind to flames.

If employees receive unsolicited e-mails containing material that is offensive or inappropriate, they must be deleted. If the employee knows the sender, they should delete the e-mail immediately and quickly inform the sender that they must not send such e-mails again. If the sender is unknown, the Chairman should be informed before the e-mail is deleted.

In addition, if employees receive jokes, video clips or games from friends via e-mail, they should delete them and not circulate them to the rest of the office. These files are often very large and can unnecessarily increase the used capacity on the server, slowing down the system for everybody.



Employees must not commit SALSC to any form of contract when using e-mail or the Internet for personal purposes and should be aware that both communication media are disclosable for the purposes of legal action. It is accepted that e-mail is routinely and properly used for minor contractual commitments such as ordering publications and data. Subscriptions to news groups and mailing lists are only permitted when the subscription is for a work related purpose. All other subscriptions (e.g. joke of the day, personal interest information) are strictly forbidden.

Blocked Sites

Although it is possible for SALSC's ICT Team to bar access to certain inappropriate websites, the Internet grows so rapidly that it is impossible to automatically prevent all inappropriate access. Employees are strictly forbidden to access any site deemed to be inappropriate by SALSC, including but not exclusively, pornography, betting/gambling sites, and "hate" sites. SALSC's Disciplinary procedure, including the Appeals Procedures built into it will ultimately determine what is 'inappropriate' in specific cases.

However, the organisation is aware that occasionally, employees may access such sites by mistake (for example, during a legitimate search). Employees who do so should inform the Chairman of their mistake as soon as practicably possible. In addition, SALSC employees are advised that it is strictly forbidden to download any offensive, obscene or indecent material from the Internet. This includes both text and images.

Good Practice

As already indicated, the need to maintain standards and adhere to SALSC policies when using e-mail or the Internet is crucial. However, for clarity, a number of the most important good practices are highlighted here.

One potential problem with browsing the Internet, even for business use, is that it can become unfocused and time consuming. This can waste employee's working time and, even when it is done in his or her own time, it ties up resources and slows down the systems. Employees should remain focused on the information they are searching for and are encouraged to contact the Chairman to discuss ways in which they can search more effectively.

Employees should disconnect after each Internet session and re-connect as required. It is not effective to remain connected for lengthy periods of time as it slows down systems.

Another problem of the Internet is that it is an unregulated source of information and so information on some sites may be inaccurate (unintentionally or otherwise). Once again, employees should seek guidance from the Chairman if they have any concerns regarding the information they have obtained.

As with all the organisation's systems, employees are responsible for good housekeeping of their own e-mail and Internet files. E-mail boxes should be cleared out regularly and only e-mails essential to effective working should be kept.

Monitoring



SALSC reserves the right to monitor both e-mail and Internet usage subject to the rules of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These Regulations authorise businesses to carry out monitoring for certain purposes provided reasonable steps are taken to inform employees that monitoring will take place and what may be checked during this process.

SALSC will monitor Internet and e-mail usage for the following reasons:

- Record keeping purposes
- Checking compliance with regulations
- Quality control
- Employees training
- Preventing or detecting crime
- Investigating or detecting unauthorised, inappropriate or excessive use
- Checking for viruses or other threats to the system

Appropriate email correspondence with Children and Vulnerable Adults

It is the responsibility of SALSC to ensure that all people associated with SALSC follow appropriate rules when emailing children or vulnerable adults.

It is inappropriate for coaches etc to email minors directly and all correspondence should be made through parents or appropriate guardians to ensure there is no opportunity for inappropriate behaviour, or the perception of inappropriate behaviour.

If there are any concerns regarding email contact with children or vulnerable adults the Chairman should be advised immediately.

Disciplinary Procedures

SALSC considers the procedures and recommendations contained within this policy to be extremely important to the efficient and lawful operation of the organisation. Any employee suspected of making inappropriate use of e-mail or the Internet will be subject to formal investigation and subsequently, disciplinary action may be taken against them in accordance with SALSC's Disciplinary procedures. In certain circumstances, breach of this policy may be considered gross misconduct and consequently may result in summary dismissal.



APPENDIX C

RECOMMENDATIONS FOR 2010

1. SALSC will review this strategy on an annual basis
2. SALSC will carry out a yearly audit and may buy up to a maximum of one day's ICT support / consultancy for this purpose.
3. SALSC will carry out a yearly risk assessment of ICT.
4. SALSC to investigate purchase of a digital video camera
5. SALSC to investigate preparation / copying of information stored on DVD / CD
6. Investigate answering system for phone calls