Internet and email acceptable use policy

1.0 Introduction

South Lakeland District Council recognises that its employees all need to use email and the Internet, they have become essential parts of our jobs. But using these tools has some inherent dangers and employees need to use them responsibly.

This policy describes relevant good practice, and it explains what the responsibilities are.

2.0 Scope of the policy

This policy is intended for all employees, temporary and contract staff (including agency staff) of South Lakeland District Council who use the Internet or email facilities.

You will only be given access to use Internet and email facilities after you have signed the authorised user agreement.

3.0 Principles

Access to the South Lakeland District Council network is subject to your acceptance of the Information Security Policy. This document is related to that policy, and it describes in more detail the benefits and responsibilities that go along with using email and the Internet at South Lakeland District Council.

4.0 Email

4.1 Personal use

With regard to personal use of email, you should treat it like the phone. You can send personal email but keep it short, don't send many, and do it in your own time. Any personal email accounts must not be used for official council business, apart from if required in an emergency situation.

4.2 The legal status

The legal status of an email is similar to any other form of written communication. This means that anything you send using council equipment can be considered to be an official communication from the council.

4.3 Controls

Given the availability for personal use, and in order to ensure that the council is protected from the misuse of email, the following controls will be exercised:

- You must comply with the instructiuons in this policy
- Don’t think of email as any less formal than a memo or letter. When sending external email take care not to include material, which would reflect poorly on the council's reputation or its relationship with clients, business partners or the general public
- Never send or store images or text (either internally or externally), which is defamatory, obscene, offensive, abusive, threatening, defamatory, risqué, in poor taste, or which could reasonably be anticipated to be considered inappropriate
- Never send or store ethnic, sexual-preference, or gender-related slurs or jokes
- Don’t send electronic chain letters
- If you aren’t sure about the appropriateness of any material, then the chances are high that you shouldn’t send it
- Treat colleagues with dignity and respect
- Don’t use email for gossip

4.4 Email security

Email isn’t secure. Sending an email is a bit like sending a postcard - anyone can read it. So if you need to send confidential material use other encrypted media, or secure email. You can send secure to other Local Authorities and Central Government via GCSX (Government Connect).

4.4.1 Be careful about clicking on links or opening attachments in emails. It is safest to only do this when you know who sent the link or attachment. Links may lead to phishing sites, and attachments may contain malware.

4.4.2 Please avoid using global lists of email addresses; these should be reserved for exceptional situations. Everyone has more email to deal with than they would like, so it helps to target only the people who really need to receive an email.

4.4.3 Email takes up space on the servers, which costs money so you should delete any email that is no longer required. It is a good idea to file any important attachments that you want to keep in your file system, rather than leaving them in Outlook. Attachments consume by far the largest amount of space.

4.4.4 When out of the office for more than a day or so, set up an ‘out of office’ rule so that people know not to expect a reply. IT Services can help if you are unsure of how to do this.

4.4.5 You should be aware that deletion of email from your account does not necessarily result in permanent deletion from the council's IT systems.

4.4.6 Email and attachments may need to be disclosed under the Data Protection Act 1998, further information regarding this can be obtained from the Data Protection Officer.

4.4.7 If you receive any email that could be considered offensive, bring it to the attention of your line manager. Incoming email is monitored and anybody who consistently sends nuisance email (including email with large attachments) to the council will have their communications bounced back to the management of the organisation that it came from with an accompanying message. That email address will also be blocked from council systems.

4.4.8 Do not supply the council's banking details to any person or organisation without prior authorisation from Finance.

4.4.9 Provided that an external party reasonably believes that someone has the authority to negotiate, or enter into, an agreement, subsequently the council will be bound by what that person has said. Email sent by authorised users will usually be acknowledged as originating from the council, so recipients will in most cases be acting reasonably if they assume that the emails are sent with the council's authority. Consequently authorised users must exercise particular care in this area of work.

4.4.10 Where organisations accept orders for goods and services via the Internet or by email the facility may only be used provided it complies fully with the council's Financial Regulations and all existing creditor payment authorisation procedures.

5.0 Internet

The council encourages the use of the Internet as an efficient form of communication and research.

5.1 You can make personal use of Internet facilities at the discretion of your line manager. Such use must be made in your own time. The council will not be liable for any loss of personal data or information as a consequence of such use. Acceptable personal use includes:

- Ordering goods online
- Personal banking
- Personal email accounts (not to be used for official council business apart from in an emergency situation.)
- Accessing websites for things like sports, TV, holiday, travel, insurance, weather, etc
- Social networking

5.2 For your own security, don't save any passwords for such sites on your PC.

5.3 The Internet may not be used for political activity, particularly the expression of support for any particular party, candidate or policy in a General, Local or European election or in any referendum.

5.4 Don't post anything related to work issues on public sites without prior approval and do not post any material, which would reflect poorly on the council's reputation or its relationship with clients, business partners or the general public.

5.5 Misuse of Internet facilities will be a disciplinary matter and will be dealt with under the appropriate Disciplinary Procedure. Misuse includes, but is not limited to, the following:

- Visiting, viewing, transmitting or downloading any material from any web site containing sexual or illegal material, or material which could reasonably be considered as offensive. If you accidentally access such a site, you must inform your line manager immediately. Failure to do so may be classed as a disciplinary offence. The publication of obscene material is a criminal offence, and the definition of "publication" includes electronic storage or transmission. If you know of employees who are visiting harmful or offensive sites, you should report that use to a Chief Officer or the IT Services Manager
- Bullying or harassment
- Personal use of Internet facilities not conducted in your own time
- Conducting any commercial activity other than ordering personal goods and dealing with personal finances

- Downloading any copyrighted materials without the permission of the copyright holder
- Downloading or installing any software without the prior approval of IT Services. IT staff may download and install software as long as it is work-related
- Wasting the council’s computer resources, for example by downloading audio, video, photographs, or other large files that are for personal use
- Using the Internet for gambling, online gaming, accessing private chat rooms, or dating
- Modifying any council PC or web browser software to enable the user to dial directly into any ISP and bypass the security precautions in place
- Originating or distributing chain letters, junk email or similar correspondence
- Jeopardising the security of the network by disclosing or sharing passwords and/or impersonating others
- Gaining or attempting to gain unauthorised access to any computer system of the council or any other organisation or hack into another website
- Any breach of relevant legislation such as the Computer Misuse Act
- Accessining peer-to-peer sharing sites

The council maintains the right to prohibit access to any particular site or newsgroup, as it feels fit to protect the interests of the Authority.

6.0 Monitoring

Whilst respecting the privacy of authorised users, the council maintains the right to monitor and audit the use of email and Internet facilities by authorised users to ensure adherence to this policy. In particular the council may log the URL (address) of each website visited and the date, time and duration of each visit.

The council may also monitor the email addresses to which emails are sent (or from which they are received) and again, the dates and times emails were sent or opened. Exceptionally, where it is considered that there are reasonable grounds to do so, the Security Officer (Infrastructure Manager) may open and read employees' emails.

Any emails sent using the government connect secure email system may be intercepted and monitored for lawful purposes.

Appendix to this document

Appendix A Authorised User Agreement

Human Resources Group: Approved July 2012