IAPF01

Internet, Email and Telephones Acceptable Use Policy

Purpose

This policy is part of the council's information assurance framework and establishes the requirements necessary for the council to implement its strategic objectives for the acceptable use of the internet, email and telephones in accordance with the Information Governance Policy.

Internet, email and telephone facilities are used by the council to support its business activities and the use of these facilities is determined by the business requirement they are intended to support.

The specific objective of this policy is to define standards that facilitate the responsible and ethical use of internet, email and telephones in a way that supports the work of the council.

Standards are required so that the council can meet its obligations under the Data Protection Act 1998 and other legislation and to meet its commitments to partner organisations and members of the public regarding the custody of information.

The standards defined allow for the establishment of effective, risk based procedures and guidelines for implementing information assurance and reinforce the council's commitment to ensuring that its information assets are protected and secure.

Scope

This policy applies to all employees, partners and, as appropriate, third party staff engaged on council business and who have access to information assets and associated systems.

The council's internet, email and telephone facilities are only intended for limited private use. The definitions of unacceptable use contained within Appendix A of this policy will still apply.

Appendix B of this policy defines the Trade Union use of internet, email and telephones.

Private use facilities are available via the Peoples' Network in Libraries and Internet Cafés on certain council premises. This policy does not apply to these facilities.

Risk Assessment

The main categories of risk within the council are:

- Emerging issues affecting the council and its services.
- New projects and service developments.
- Current issues or developments within the council's existing services.
- Monitoring of performance measures.
- On-going provision of the council's services.

The Information Governance Policy defines how the management of each risk category should be evidenced and each category should be considered in applying appropriate standards for the acceptable use of internet, email and telephones.

Managers must ensure that standards which reflect this policy are in place and that staff are aware of the reasons for these and the expectations around compliance.

Standards

All users must agree to adhere to this policy by accepting the provisions contained within the Employee Agreement for the use of council internet, email and telephones in the manner approved at the time of application. Without this agreement access will not be provided.

Internet, email and telephone facilities will be provided only where they are required to carry out official duties.

At no time must these facilities be used in ways which are considered unacceptable by the council, unless specifically approved for business purposes. Appendix A defines what the council considers as unacceptable use.

The Fair Use Policy for Mobile Phones issued by One Connect Limited on behalf of the council must be followed for the use of all council issued mobile phones.

All use of internet, email and telephone facilities may be monitored by management and records examined without reference to individuals.

All messages and transmissions generated using these facilities are regarded as the council's property and responsibility and all associated emails and records will be treated as business records. Private, non-business email will generally be treated in the same way as business email and monitored, handled and archived as such and cannot therefore be regarded as private in all circumstances.

Business emails containing personal or sensitive data must be sent using the corporate email encryption product, the Government Connect secure email services or, through specific SIRO approved arrangements already in place.

Comments contained in email or posted to any other system visible on the internet will not necessarily be considered by the council as formal statements issued by, or the official position of, the council and should not be phrased as such. A disclaimer appears on all outgoing emails.

Council rules and conventions which govern the disclosure of personal and other sensitive data and the expression of opinions about the council or service users in public areas continue to apply if you use Web 2.0 services, such as Facebook, in your personal capacity outside work.

The council permits some non-business use of the internet and email but only during personal time. These facilities have been configured for business purposes and so there are some inherent limitations on personal use. All use for personal purposes remains subject to acceptable use rules relating to purposes and content as outlined in Appendix A.

The use of internet, email and telephone facilities for communication with union representatives or employee-relations reasons and essential communication with home for co-ordinating work and family life are within the definition of business use and are therefore acceptable.

The limitations on email use are greater as personal and professional internet personas should be kept separate. Your business email address must not be used for non business purposes. Exploitation or uses of Internet services which go beyond this basic level, although they may be initiated by anyone, must be approved on a business case basis through line management. This means that council email addresses may only be used in a personal capacity when communicating with the union and home or family in the way described above.

During working time, an individual's use of internet, email and telephone without reference to management is limited to business purposes. This excludes social media sites such as Facebook unless a specific business case has been approved.

Council owned mobile phones etc. must not be used whilst driving.

Council supplied SIM cards must only be used in council supplied devices.

References

Data Protection Act 1998

Code of Conduct for Employees
http://lccintranet2/corporate/web/view.asp?siteid=2859&pageid=5795&e=e

Human Rights Act 1998

OCL Fair Use Policy for Mobile Phones -
http://lccintranet2/corporate/web/view.asp?siteid=2859&pageid=39181&e=e

The council's information assurance policy framework is designed to provide a layered approach to information security and assurance, ensuring that suitable precautions are adopted in all situations. Individual policies should not be considered in isolation but rather as elements of the whole.

Governance and responsibilities

All Managers are responsible for ensuring that relevant policies and supporting standards and guidance are built into local processes and that there is on-going compliance on a day to day basis. Any breaches or suspected breaches of confidentiality or information security must be reported in accordance with the Security Incident Management Policy.

If circumstances arise which mean that this policy cannot be followed or is required to be varied for business reasons, employees and contractors must obtain authorisation for an alternative procedure from the relevant Director, in consultation with CIGG.

There is an exception list that will be maintained within this policy and agreed by CIGG.

All Managers are responsible for the identification of existing or emerging information risks relating to their service area and either addressing or reporting the issues to CIGG for consideration. Where risks cannot be addressed locally, or require input from another party, e.g. One Connect limited, they should be reported in accordance with the Security Incident Management Policy to ensure the issue can be considered by CIGG.

All staff, including permanent, temporary, contractors and any individual who has been given access to the council's network, systems or other information are personally responsible for the content of all text, data, audio or images that they place on or send over the council's internet, email and telephone facilities and must comply with this policy and are expected to report non-compliance or weaknesses to their line manager or in accordance with the Security Incident Management Policy if appropriate.

Compliance

Non-compliance with this policy could have significant effects on service delivery and may adversely impact individuals, waste resources and cause reputational damage to the council.

The SIRO and CIGG are responsible for ensuring overall compliance with the Policy.

An individual’s use of corporate ICT facilities may be monitored by management and records examined without reference to the individual, to ensure compliance with policy, prevent crime and maintain system performance.

The council's code of conduct for employees sets out the behavioural standards that must be upheld by all employees of the council and forms part of the council's terms and conditions of employment.

Compliance with this policy is mandatory. Non compliance may result in action being taken under the council's Disciplinary Procedure and could result in dismissal from employment with the council.

A breach of policy involving a partner or third party organisation will be treated as a security incident and investigated in accordance with the Security Incident Management Policy. Appropriate action will be agreed with the SIRO taking into consideration any specific contractual recourse or sanctions available.

Definitions

Web 2.0 websites provide increased user-interface, software and storage facilities than traditional static web pages and the terms is generally associated with social networking and user created web sites

IAPF01

Internet, Email and Telephones Acceptable Use Policy

APPENDIX A

Unacceptable uses of council internet, email and telephone facilities

Any use that is illegal, against council policy or contrary to the council's best interest, particularly:

- If it is a non-council business use and for an unacceptable purpose.
- If it is a frequent and/or time consuming non-business use of internet, email or telephones.
- If it contains unacceptable types of content.

Unacceptable purposes

Examples of non-council business use of the internet, email and telephone facilities which are unacceptable at any time, include but are not limited to:

Any use associated with running a business activity, whether for profit or not.

Any type of private, business or financial transaction including gambling & barter.

Shopping, and other personal financial transactions, including examples such as banking, operating a wedding present account with a store, placing orders for goods or services, auction sites.

Expressing personal opinions, expressing political views and breaching conditions of politically restricted posts.

Computer crimes, such as hacking.

Harassment of any kind.

Downloading music and films.

Any use of internet facilities which would allow unacceptable non-business use of LCC systems to be concealed.

Accessing sites which are blocked for reasons of legality or taste without approval

Using your work email address for personal purposes, such as:

- subscribing to email newsletters which are not work related;
- using as a contact address on websites e.g. selling goods and services;
- use of social media web sites such as Twitter and Facebook;
- uploading photographs and information to web sites such as Flickr and Wikipedia;
- online auction activity, for example, eBay transactions;
- producing publications for sale;
- creating web pages and blogs;
- frequenting chat rooms, discussion forums and personal messenger services;
- Peer to peer exchanges.

Frequent and/or time consuming non-business use

Frequent non-business use of internet, email and telephone facilities should not take place in work time. Examples, which may be non-essential business uses, perhaps occurring as a result of unsolicited emails, include, but are not limited to:

Excessive visits to sports results, commentaries and news sites.

Personal non-council business distribution lists greater than 5 addresses.

Bulk personal internal or external emails.

Participating in chain letters and petitions.

Sending non-council business emails with large attachments.

Chatting or distributing jokes via email or text.

Unacceptable content

Some types of content that are unacceptable may be accessed or copied from websites or be contained in emails and messages as text, graphics or sound. Examples are:

Content that brings the council into any kind of disrepute.

Content that infringes copyright.

Content that may be construed as discriminatory, offensive, defamatory, or obscene.

Content that is derogatory about an individual's race, age, disability, religion, national or ethnic origin, physical attributes or sexual life.

Content that contains abusive, profane or offensive language.

Content that contradicts council values of respect for all and promoting shared values and safer communities, e.g. content that promotes hate incidents or hate crime.

IAPF01

Internet, Email and Telephones Acceptable Use Policy

APPENDIX B

Trade Union use of internet, email and telephone facilities

The main policy applies to union users of the council internet, email and telephone facilities. The following provisions also apply specifically to trade unions.

Use of these facilities by members of a recognised trade union for communication with union representatives, union officials or other members on matters of union business or employee-relations reasons are regarded as coming within the definition of business use and are therefore acceptable.

Use of these facilities to encourage staff to act inappropriately or against the best interests of their employer would fall outside this definition.

Accredited trade union representatives may use council internet, email and telephone facilities to support their role in whatever aspect Examples include union learning representative, health and safety representative or equality representative.

On-line financial transactions which the union undertakes in the course of its business which relate to matters such as rail and air travel for stewards and officers, hotel accommodation and conference/seminar places and the purchase of items from various suppliers for branch and promotional use, will be treated as any other council business internet and email traffic and the use by unions of these facilities for these purposes is at their own risk.

It is accepted that unions may use social media for union business to the extent that it is technically allowed on the council network.

Trade union membership details are classified as sensitive personal data under the Data Protection Act and use of email must be carried out in such a way that members' names are not disclosed to third parties without consent. Bulk emails must be sent using blind copying.

IAPF01

Internet, Email and Telephones Acceptable Use Policy

APPENDIX C

Misuse of email – Disciplinary offenses

This document explains how the misuse of your council email account would lead to a breach of the policy and to possible disciplinary action.

An explanation of what is considered inappropriate content and rules for the personal use of email are contained in the policy Appendix A.

There are also standards to apply if you receive email that may lead to a breach of the policy.

It is important to understand that under the Officer Code of Conduct a serious violation of this policy could be regarded as gross misconduct and could result in your dismissal from employment for a first offence.

Any form of harassment or bullying, either face to face or via email would be regarded as gross misconduct.

Breaches of Policy

The distribution of images, text or materials externally that are considered inappropriate under the definitions contained within the acceptable use policy.

You must not distribute externally (to addresses outside of the council) any email that contains inappropriate content. This is the most serious violation of the policy. All email sent externally are identifiable to the council and have the potential to bring the council into disrepute.

The distribution of images, text or materials internally that are considered inappropriate under the definitions contained within the acceptable use policy.

You must not distribute internally (to council email addresses) any email that contains inappropriate content.

The import of images, text or materials that are considered inappropriate under the definitions contained within the acceptable use policy.

You must not send any email from a personal email address to your council email account that contains inappropriate content.

The soliciting of images, text or materials that are considered inappropriate under the definitions contained within the acceptable use policy.

You must not request any person(s) to send you emails that contain inappropriate content.

(If you give your email address to a business acquaintance, friend or family member you should always let them know what is and is not acceptable to send to you at work. In addition, the rules for personal email state that where you are in receipt of personal emails you should advise the sender that these may be monitored).

The storage of images, text or materials that are considered inappropriate under the definitions contained within the acceptable use policy.

You must not retain any emails that contain inappropriate content in any part of your mailbox. Each member of staff is responsible for the content of their mailbox.

The improper disclosure of confidential and/or personal information.

Paragraph 5.8 of the Officer Code of Conduct requires you to maintain the confidentiality of confidential information. The unauthorised disclosure of personal data is an offence under the Data Protection Act 1998 and a breach of the council's Data Protection Policy. These requirements must be considered in your use of email. Therefore if your email contains personal or otherwise sensitive data you must use the corporate email encryption product or Government Connect secure email services. (see intranet) You cannot use confidential or personal council information for your own purposes.

A failure to report a breach of policy.

If any member of staff sends you email that contains inappropriate content or, is in any other way in possible breach of this policy you are obliged under Paragraph 5.12 of the Code of Conduct for Employees to inform your line manager.

(If you feel unable to approach your immediate line manager you should notify a more senior manager within your service area or use the confidential whistle blowing helpline).

Document Control

Organisation	Lancashire County Council
Title	IAPF01 Internet, Email and Telephones Acceptable Use Policy
Author	Ian Shipcott
Filename	
Owner	County Secretary & Solicitor (SIRO)
Subject	Information Governance
Protective Marking	Not Protectively Marked
Review date	

Revision History

Version	Status	Revision Date	Summary of Changes	Author
0.1	Draft	6/2/13	First Draft	I Shipcott

Review and Approvals

Title	Name	Signature	Date of Issue
IG Project Lead			
CIGG			
SIRO			

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version