Inverclyde council

Information Governance & Management Framework

Acceptable Use of Information Systems Policy

Version 1.3

Produced by:

Customer Services & Business Transformation
Inverclyde Council
Municipal Buildings
GREENOCK
PA15 1LX

17/03/2010

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER

THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.

DOCUMENT CONTROL

Document Responsibility		
Name	**Title**	**Service**
	Inverclyde Council Information Systems Acceptable Use Policy	CS&BT

Change History		
Version	**Date**	**Comments**
0.1		
0.2	27/12/2006	RS – changes as per meeting 11/12/06
0.3	10/5/07	RS – Laptop physical security measures
0.4	14/5/07	RS – format changes
0.5	29/5/07	RS – Extended para 2 – section 1 + added music/video streaming SW
1.0	25/10/2007	Final version for approval by committee
1.0	21/11/2007	Approved version – P&R 20/11/2007
1.1	20/01/2010	Added Appendix 1 for GSx – Personal Commitment Statement
1.2	19/02/2010	Information added wrt removable storage media
1.3	17/03/2010	Inclusion of consultation with Information Governance & Management Working Group

Distribution		
Name	**Title**	**Location**
Corporate Directors & Heads of Service		

Distribution may be made to others on request

1. General Principles

This policy applies to all Council employees and elected members and covers the use of the Internet and email, as well as equipment security and working from home on Council business.

NB Staff authorised to use GSx/GSi accounts should note the detailed contents of the GSx/GSi Personal Commitment Statement contained within Appendix 1.

Information and Communications Technologies are an integral part of the business of Inverclyde Council. The Council gives access to ICT systems, email and the Internet to relevant employees, in order to enhance their ability to perform their duties. The Council will always endeavour to be as flexible as it can be in allowing a reasonable level of personal use of email and the Internet and such use by employees should always be outwith core hours. However, should this right be abused, the Council reserves the right to withdraw personal use without notice.

How employees communicate with people reflects on the individual and on the Council as an organisation. The purpose of this policy is to ensure that all employees: -

- understand what is and is not acceptable use of ICT systems, especially email and the Internet
- are aware that all electronic communications are monitored and logged
- understand that, under the Freedom of Information Act (2002), all files and communications may be released to the public
- understand the implications of inappropriate use of ICT systems
- Notwithstanding the above, all employees understand that their rights to privacy will be respected

All information relating to customers and Council operations is confidential. All employees ***must*** treat the Council's paper-based and electronic information with utmost care.

Downloading, copying, possessing and distributing material from the Internet (or any other source) may be an infringement of copyright or other intellectual property rights. Therefore, in general, employees ***must not*** download or copy any material onto Council ICT equipment, unless the information is clearly for business purposes.

Whilst ICT systems are provided primarily for business use, the Council will allow occasional personal use, at the discretion of the employee's line manager, provided that this use does not: -

- conflict with work or business activities
- violate any Council policies or law
- involve any inappropriate content
- involve any use for personal entertainment
- involve the use for any business purpose, other than that of the Council
- involve the ordering of any goods/services over the Internet, other than approved goods for business use. (e.g. Personal banking, payment of bills, booking of personal, non business flights etc)

Employees may be asked to justify the amount of time they have spent on the Internet, or the sites they have visited or the level of personal use of email. Failure to provide a satisfactory explanation may result in disciplinary action, under the Council's disciplinary procedures.

The Council will respect all employees' rights at all times and also places a level of trust in its staff to use these facilities professionally, lawfully, consistently with their duties and with respect for colleagues.

Employees who do not follow the guidelines in this policy may be liable to disciplinary action, under the Council's disciplinary procedures.

In addition to invoking the disciplinary procedure, the Council reserves the right to restrict or deny access to email or the Internet to any employee at work and, in such cases, will give reasons for doing so.

Any employee who is unsure about whether something he/she proposes to do might breach this e-mail and internet policy or is proposing to do something not specifically covered in this policy should seek advice from his/her manager and/or Customer Services & Business Transformation.

2. Monitoring of Communications

The Council will exercise the rights and obligations of a data controller under the Data Protection Act 1998 in relation to staff communications.

The Council has a responsibility to both its employees and the organisation to ensure that ICT systems, email and Internet access are used in a safe, legal and businesslike manner.

In order to ensure the above:-

- all email communication, including incoming and outgoing personal email, and Internet access is monitored at all times and logged automatically by ICT systems
- all emails are filtered for inappropriate language, content and attachments
- ICT systems automatically prevent access to Internet sites that are deemed inappropriate, because of content or because of the security implications of the technology used within the site.

From time to time, there may be circumstances under which it may be necessary for the Council to retrieve and use this recorded information. Whenever this is the case, the Council will endeavour to inform an affected employee when this is to happen and the reasons for it.

Examples of circumstances under which it may be necessary to examine this information include the following:-

- If the Council suspects that the employee has been viewing or sending offensive or illegal material. (e.g. racist, sectarian, nudity etc)

- If the Council suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications or spending an excessive amount of time viewing websites that are not work related.

- If the Council suspects that the employee is sending or receiving e-mails that are detrimental to the Council

Where an employee is absent through illness or on annual leave, the Council may require to open emails sent to the employee. The opening of emails in these circumstances ***must*** be authorised by the Head of Customer Services & Business Transformation, the employee's Head of Service in consultation, where appropriate with the Head of Legal & Administration.

3. Use of Council ICT Equipment

Employees ***must*** take reasonable care of all ICT equipment issued to them. Basic security guidelines for staff using Council owned equipment include:-

- Store laptops out of sight. If a laptop is used as an office desktop machine, it ***must*** be removed from the desk and stored securely overnight, in a locked drawer or cupboard.

- Rotate storage locations, if possible, of laptops. Changing patterns can make it harder for thieves to prepare for the theft.

- The Council will supply an appropriate carrying case or backpack for transporting the laptop safely and inconspicuously.

- Keep the laptop close at hand. Staff should not leave the laptop case unattended, even for a short time. If possible, remain in physical contact with it at all times.

- Whilst travelling by car, staff ***must*** ensure that the laptop is locked out of sight in the boot of the car, to prevent opportunistic theft.

Employees ***must not***

- connect Personal Digital Music/Video Players to their Council PC

- install or use music or video streaming software, except where express permission has been given by the Head of Customer Services & Business Transformation

- store MP3/WMA (or similar) files, AVI/MP4 (or similar) video files on their local or network drives. They may not use the council network to distribute such files. (Where Services require to utilise such files with respect to providing training or other purpose, prior approval from the Head of Customer Services & Business Transformation ***must*** be obtained.)

- download, install or store games, screensavers and/or wallpapers from the Internet or from any other source

- use Council ICT equipment for any other business purposes, other than those directly related to the Council

- use these facilities to operate any business and/or service operated by them or a third party

- make any attempt to circumvent network security restrictions

- take equipment home or move equipment without permission of their line manager.

4. Use of Electronic Mail

Employees should expressly agree with the recipient, wherever possible, that the use of email is an acceptable form of communication, bearing in mind that if the material is confidential, privileged, price sensitive or commercially sensitive, unencrypted email is not secure.

Some intended recipients may have rigorous email gateway protocols (or firewalls), which can automatically screen all incoming email for content and source. If this is the case, consider whether this means of communication is appropriate.

Employees ***must not***: -

- send or forward messages which are defamatory, libellous, obscene or otherwise inappropriate. The use of email in this way will be treated as misconduct under the Council's disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

- forward any obscene or defamatory email, whether received unwittingly or otherwise and from whatever source, to any other address.
- impersonate any other person when using email or amend any messages received
- open unsolicited email
- open any attachments from unknown senders
- respond to or forward any chain emails
- forward social emails from friends and colleagues
- click on any unknown or suspicious embedded links.

All email communication is monitored and filtered for inappropriate language, content and attachments. Suspicious emails are quarantined and intended recipients within the Council are sent a message detailing the content and ***must*** give approval before the email is released. If the recipient does not wish to receive the message it is automatically deleted. Details of all quarantined messages are retained. Where it cannot be established by Customer Services & Business Transformation that an email or an attachment to an email presents no risk to the Council Network under no circumstances will that email be released.

5. Use of the Internet

When using an Internet site, employees ***must*** always read and comply with the terms and conditions governing its use.

Employees are ***specifically prohibited*** from downloading and installing software without authorisation from Customer Services & Business Transformation. Any such requests will be judged on whether the software fulfils a business requirement that cannot be provided from the range of software already provided and supported by Customer Services & Business Transformation. Customer Services & Business Transformationwill check that the source is safe before allowing installation. Customer Services &

Business Transformationis also responsible for keeping a record of the licences for all software used in the Council, whether the software was free or paid for. Employees may not download software for non-business related purposes.

Employees are expressly prohibited from: -

- downloading any material that is copyright protected unless authorised to do so by the copyright owner
- downloading any images, text or material which are obscene or likely to cause offence (e.g Racist, sectarian, nudity etc)
- downloading any such material not required solely for business purposes
- introducing any software which has not been authorised (either from on-line or other sources)
- ordering any goods/services over the Internet, other than approved goods for business use
- seeking to gain access to restricted areas of the network
- knowingly seeking to access data which they know or ought to know to be confidential unless authorised to do so
- introducing any form of computer viruses
- carrying out any “hacking” activities
- opening any email via Web Mail accounts. Eg Hotmail, Yahoo Mail, AOL, NTLWorld etc. unless authorised to do so.

For information, the following activities ***are criminal offences*** under the Computer Misuse Act 1990: -

- Unauthorised access to computer material ie hacking
- Unauthorised modification of computer material
- Unauthorised access with intent to commit/facilitate the commission of further offences

Customer Services & Business Transformationhave implemented filtering software that prevents access to sites that are deemed inappropriate because of content or because of the security implications of the technology used within the site. This software monitors and logs all sites visited by

council employees and employees are directed to a warning page when a blocked site is accessed.

Where staff are involved in creating, amending or deleting the Council's web pages or content on the Council's web sites, such work should be consistent with their responsibilities and be in the Council's best interests. Employees ***must*** always ensure that the proper vetting procedures have been complied with and the information is accurate and up-to-date.

6. ICT Systems Security

Employees ***must***: -

- not use ICT systems in any way that may damage, overload or affect the performance of the system or the internal or external network.
- ensure that all confidential information is secure and used only for the purposes intended and is not disclosed to any unauthorised third party.
- keep their user names and passwords confidential at all times.
- ensure that they lock their computer whenever they move away from it for any length of time (Press Ctrl-Alt-Delete simultaneously then click Lock Computer. This will ensure that the machine can only be unlocked with the original password.)

7. Remote and Home Working

This section applies to the use of Council laptops and PCs when accessing Council systems from outwith Council premises. e.g. Home access

Where employees have been given the facility to access the Council Network from home, or any other remote location, they will be provided with a Council owned Laptop or Desktop PC. Employees are not permitted to access the Council network remotely with their own equipment.
It is anticipated that very few staff should have a permanent requirement for a USB memory device, those who do will be issued with a council owned and managed device only after their requirement has been approved at service manager level or above and with the agreement of the Head of Customer Services & Business Transformation. Individuals will be fully responsible for the safe use and management of these devices and the consequence of any data loss should be understood and acknowledged.

Where a temporary requirement for a USB memory device is identified, the ICT Servicedesk will issue a device from a centrally held stock. It will be issued for a fixed period of time and only for the purposes identified in the request. Again the

Individual will be fully responsible for the safe use and management of this device and the consequence of any data loss should be understood and acknowledged.

Use of Council owned laptops and PCs is covered by Display Screen Equipment Regulations 1992. A Display Screen Equipment Assessment is required and a home visit may be carried out by the Council's Health and Safety Officer to ensure home workstations comply with the requirements of the regulations.

All employees ***must***:

- password protect any work which relates to the Council's business
- position themselves so that work cannot be overlooked by any other person
- take reasonable precautions to safeguard all passwords and the security of any computer equipment on which they do the Council's business
- apply an appropriate level of security to any personal data which comes into their knowledge, possession or control through their employment with the Council, so that the personal data is protected from theft, loss, destruction or damage and unauthorised access and use
- inform the police and Customer Services & Business Transformationas soon as possible, if a laptop in their possession or any computer equipment on which they do the Council's work has been stolen
- ensure that any work which they do remotely is saved on the Council's network or transferred to the Council's network as soon as reasonably practicable.

8. Data Protection

On occasion, Council employees may possess or control personal data. When in possession of such personal data, employees ***must***: -

- keep the data confidential and not disclose any information to any other person unless authorised to do so by the Council
- familiarise themselves with the provisions of the Data Protection Act 1998 and comply with its provisions
- process personal data strictly in accordance with the Data Protection Act 1998 and other policies and procedures issued by the Council
- not make personal or other inappropriate remarks about clients or colleagues on manual files or computer records, since the subject of

such remarks has a right to see information the Council holds on that individual.

Inverclyde Council views any breach of the Data Protection Act 1998 and its data protection policy as gross misconduct which may lead to summary dismissal under its disciplinary procedures.

If an employee makes or encourages another person to make an unauthorised disclosure knowingly or recklessly, they may be held criminally liable.

Appendix 1 GSx/GSi Personal Commitment Statement

I understand and agree to comply with the security rules of my organisation as well as the GSi Code of Connection as explained to me in security awareness training I have received.

For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include: -

I acknowledge that my use of the GSi may be monitored and/or recorded for lawful purposes; and

- I agree to be responsible for any use by me of the GSi using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and
- will not use a colleague's credentials to access the GSi and will equally ensure that my credentials are not shared and are protected against misuse; and
- will protect such credentials *at least* to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and
- will not attempt to access any computer system that I have not been given explicit permission to access; and
- will not attempt to access the GSi other than from IT systems and locations which I have been explicitly authorised to use for this purpose; and
- will not transmit information via the GSi that I know, suspect or have been advised is of a higher level of sensitivity than my GSi domain is designed to carry; and

- will not transmit information via the GSi that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and
- will not make false claims or denials relating to my use of the GSi (e.g. falsely denying that an e-mail had been sent or received); and
- will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GSi to the same level as I would paper copies of similar material; and
- will not send protectively marked information over public networks such as the Internet; and
- will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain; and
- will not auto-forward email from my GSi account to any other non-GSi email account; and
- will disclose information received via the GSi only on a 'need to know' basis; and
- will not forward or disclose any sensitive or protectively marked material received via the GSi unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and
- will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GSi (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted; and

- will securely store or destroy any printed material; and
- will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GSi (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc., so as to require a user logon for activation); and
- where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection; and
- will make myself familiar with the security policies, procedures and any special instructions that relate to the GSi; and
- will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and
- will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and
- will not remove equipment or information from my employer's premises without appropriate approval; and
- will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief); and
- will not introduce viruses, Trojan horses or other malware into the system or GSi; and
- will not disable anti-virus protection provided at my computer; and

- will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and
- if I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

Enter Name: Gordon McLoughlin **Position**: Risk Owner

Date: 20th January 2010

for and on behalf of all users at: Inverclyde Council
(Connecting organisation)