West Dunbartonshire Council

Corporate Resources - Finance & ICT

Corporate Information and Communication Technology Security Policy (ISP - 4.7)

Last Updated March 2010

Index

Appendix

1 Introduction

1.1 The Council has a large investment in the use of Information and Communication Technology (ICT) which is used to the benefit of all departments and other agents. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level which is appropriate for the Council's needs.

Examples of ICT are as follows

- PC's, Laptops,& Netbooks
- Windows & UNIX Servers
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Mobile Phones/smart phones
- Radio Equipment
- Personal Digital Assistants (PDA)
- Tablet Devices
- Memory Sticks

1.2 To help maintain equipment, systems and data in a secure environment, there are a number of requirements to be observed. These requirements are defined in this document.

2. Policy Objectives

2.1 The main objectives of this policy are:

- To ensure that all of our Council's assets, staff, data and equipment are adequately protected on a costeffective basis against any action that could adversely affect the ICT services required to conduct our business;

- To ensure that staff are aware of and fully comply with all relevant legislation; and

- To create and maintain within all departments a level of awareness of the need for ICT security to be an integral part of our day to day operation so that all staff understand the need for ICT security and their own responsibilities.

3. Application

3.1 The security policy is relevant to all ICT services irrespective of the equipment or facility in use and applies to:

- All employees;
- Employees and other agents of other organisations who directly or indirectly support or use the ICT services;
- All use of ICT throughout the Council.

4. Responsibility for Security

4.1 'Each services'_directorate.' are responsible for the computer equipment under their control and for its proper use. ICT security is the responsibility of all members of staff. The policy has been approved and adopted by the Corporate Management Team.

4.2 The ICT security policy will apply to all corporate employees and agents who have access to computer resources using Council approved technology. All members of staff and agents will be issued with computer security instructions which will specify their responsibilities and draw their attention to the penalties for not complying with the instructions.

4.3 Senior and line managers in departments are responsible for the implementation and policing of the Security Policy.

4.4 All users of ICT services must ensure the security, integrity within the service provided.

4.5 All user departments must nominate authorised personnel who are responsible for specific systems under their control. These nominations should be recorded with the Head of Audit, Performance & Strategic Planning.

4.6 Users who have cause to come in contact with the GSx network have an additional responsibility to comply with extra security controls and must sign a personal commitment statement acknowledging this.

4.7 GSx users must be aware of their responsibilities regarding computer security with information up to and including a 'Protective Marking of Restricted' .

5. Legislation

5.1 The Council has to abide with all UK legislation and any relevant European Law affecting ICT. All employees and other agents of the Council must comply with the following Acts and they may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted:

- Data Protection Act, 1984 and/or 1998;
- Copyright Designs and Patents Act, 1988;
- Computer Misuse Act 1990;
- Freedom of Information Scotland Act 2005.
- Digital Economy Act 2010

5.2 Information and brief guidance about the above Acts is contained in an appendix to this document.

6. Standards and Procedures

6.1 Physical Access

6.1.1 Precautions should be taken to ensure that access to PCs, including laptops and netbooks, is restricted at all times to authorised personnel.

6.1.2 Equipment should be sited to reduce the risk of damage, interference and unauthorised access.

6.1.3 All computer equipment must be authorised by ICT and be recorded on both the department's establishment and Head of Finance & ICT inventories. You are referred to the Council's Standing Inventory Instructions.

6.1.4 Where computer equipment is removed from buildings, e.g. for use at an external site:

- Prior approval must have been obtained from the authorised person specifying the reason for removal and the duration. Appropriate mechanisms must be employed by management to ensure the timely return of all equipment and that no damage has occurred: and
- All of the provisions of this policy document equally apply.

6.1.5 Where computer equipment is used for home working:

- Health and Safety checks should be made at the location before using council equipment.
- Insurance liability must also be checked before council equipment is used in the home.
- Two factor authentication must be used.
- The nature of mobile and home working using council provided equipment is such that information will be viewable on the screen of the user's computer, since this information is likely to be private/confidential, users must understand their responsibilities on how to handle this type of data in a mobile/home working environment.

6.1.6 No equipment purchased, leased or hired by a user department may be connected to the network or attached to any equipment connected to the network without authorisation by ICT. This restriction also applies to any equipment not owned, leased or hired by the Council.

6.2 Software Access

6.2.1 Permission from 'Each services'_directorate.' is required in advance before a request is made to ICT to link personal computers to corporate computer systems.

6.2.2 Boot passwords should only be set on sensitive PCs, after consultation with ICT, to prevent unauthorised access to locally held software and data. Boot passwords should be held securely and accessible only to authorised ICT staff.

6.2.3 Encryption software recommended by Finance & ICT must be used on all portable devices including laptops and mobile devices.

6.2.4 PCs should not be left 'logged in' when unattended. Wherever the system allows, a screensaver providing immediate complete screen confidentiality should be used in conjunction with a password. The screensaver option has been set to activate corporately after 10 mins.

6.2.5 Passwords must be used to protect all systems and **must not be written down or disclosed to others**. **Employees and other agents may be held liable for any misuse of a computer resulting from use of their password username**.

6.2.6 Proper approved procedures are in place and will be used to notify ICT of all leavers to facilitate the prompt removal of all access rights.

6.2.7 Passwords must be specific to individual staff and comprise a minimum of eight alpha/numeric characters arranged in such a way as they will not be easily guessed.

6.3 Information

6.3.1 Information held on the Council's ICT facilities or subsequent output, e.g. printed letters/tabulations, is the property of the Council and is governed by the provisions of the Data Protection Act. Any purpose for which personal information is held about people must be registered under the Act by the Council's Data Protection Officer, who is the Head of Finance & ICT. Advice on registration can be provided by Finance & ICT.

6.3.2 Data held should only be released to authorised persons and ICT. Supplied equipment must only be used for authorised purposes. Where ICT facilities are used for authorised personal work this activity must not prejudice or interfere in any way with the Council's ICT facilities nor its service provision or activities.

6.3.3 Any personal or sensitive data displayed upon unattended equipment must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so. This is applicable to information displayed on visual display units, printed output and computer produced media such as DVD, CD and other portable media.

6.3.5 All computer output no longer required by the Council should be disposed of with due regard to its sensitivity. Confidential output should be disposed of by shredding or secure disposal by an approved agent. Individual departments are responsible for ensuring that appropriate facilities are provided.

6.3.6 Any queries relating to the provisions of the Data Protection Act and how it affects your operations should be directed via your line manager to the Head of Finance & ICT. You are directed to the provisions of ICT Procedure 1. – Data Protection for a comprehensive description of your obligations under the Data Protection Act.

6.4 Virus Protection

6.4.1 All PCs (including laptops/notebooks) should be protected by virus detection software which will be subject to regular updates to guard against new viruses. Any detected viruses must be reported to ICT immediately.

6.4.2 All disks/CD's/DVD's or potable media must be virus checked prior to use in any of the Council's computers. This especially applies where disks have been received from an external source.

6.4.3 All Computers/Laptops connected to the corporate network will have anti-virus software automatically installed. Regular anti-virus software updates will be provided by ICT.

6.5` Wireless & Mobile Working

6.5.1 All Wireless access points must comply with corporate standards as described in the Wireless device policy, be registered, have at least WPA2 encryption with relevant passwords kept with the register and super user passwords disguised, failure to comply may result in disciplinary action.

6.5.2 Users wishing to utilise authorised wireless networks must request such access via Finance & ICT (F&ICT) and identify the machine that will be used for accessing wireless networks.

6.5.3 Access of unauthorised wireless networks is prohibited (for example, McDonald's, Starbuck's, hotel's etc..) when using council provided equipment UNLESS explicitly authorised as part of the Home and mobile working initiatives.

6.5.4 Any requirement for the use of 3G modems must be agreed and procured via F&ICT

6.5.5 Use of Blackberry devices must be secured by passwords.

6.5.6 The use of Blackberry devices for Internet browsing will be subjected to the same filtering rules, restrictions, and disciplinary actions as though browsing via an office based PC.

6.5.7 The use of mobile devices for roaming or home working brings an additional security risk, all users of such services must accept that the devices will be secured by encrypting the hard disk and access by any device other than authorised, secure, memory sticks will be denied

6.5.8 Access to Email whilst roaming, must be via Council provided Blackberry devices or laptops, the purchase of these devices is controlled and managed by F&ICT.

6.5.9 The use of Smartphones to access any email accounts must be authorised by ICT prior to use.

6.5.10 The use of Smartphones to access GSX email accounts is expressly prohibited.

6.5.11 All employees and other agents using WDC Mobile Devices should note that this Security Policy applies to the usage of such Mobile Devices,. A "Mobile Device" means ; Blackberry; MDA; Smart Phone, Tablet/Laptop and any other handheld devise capable of making and receiving phone calls; Text; Emails and accessing the intranet and internet.

6.5.12 Users of wireless and mobile devices must report any suspicious activity on their machines to Finance & ICT

6.5.13 Use of webmail implies that information will be viewable on the screen of the user's computer, since this information is likely to be private/confidential, users must understand their responsibilities on how to handle this type of data when using webmail

6.5.14 The loss of, or suspected compromise of, laptops or mobile devices MUST be reported immediately to the ICT service desk

6.6 Software Copyright

6.6.1 The copying of proprietary software programs or associated copyrighted documentation is prohibited and is an offence and could lead to personal criminal liability with the risk of a fine or imprisonment.

6.6.2 The loading of proprietary software programs for which a licence is required but not held is prohibited and is also an offence which could lead to a large fine or imprisonment.

6.6.3 Deliberate unauthorised access to, copying, alteration, or interference with computer programs or data is prohibited.

6.6.4 Staff negotiating contracts, under which software is to be written/provided to the / for the Council must seek to ensure, in consultation with the Council's legal representatives, that suitable arrangements are made for the copyright to be vested in the Council or that appropriate third-party agreements are in place.

6.6.5 All computer programs and data developed for the Council are for the sole use of the Council except by permission of the Services Directorate.

6.6.6 **Personal software must not be loaded onto Council computers under any circumstances**. If the software is deemed to be of use to the Council then it should be duly acquired under licence.

6.6.7 Spot checks may be conducted by Internal Audit personnel to ensure compliance with these provisions. You should be aware that the electronic inventory software used by the Council can identify and provide evidence of unauthorised software, including games. Authorised personnel from Internal Audit have rights of access to all systems, the power to seek explanations from members of staff concerned and the right to remove any unauthorised software found to have been installed. You are referred to the Council's Financial Regulations and Defalcation Procedures, which may apply in certain circumstances.

6.7 Computer Misuse

6.7.1 All employees and other agents must be aware of their access rights for any given hardware, software or data and should not experiment or attempt to access hardware, software or data for which they have no approval or need to conduct their duties. You are referred to the Appendix accompanying this document for a summary of the Computer Misuse Act 1990 and the Data Protection Act.

6.7.2 All employees must be aware that the downloading or storage of files/data for personal use on Council equipment is prohibited. Regular monitoring will be carried out by ICT and Senior Management will be informed of personal data storage and the data/files will then be removed and can result in disciplinary action.

6.8 Contingency Planning

6.8.1 Security copies (back ups) should be taken at regular intervals dependant upon the importance and quantity of the data concerned. In the case of systems operating on the corporate communications network these will be taken on behalf of users by ICT as part of their routine backup schedule.

6.8.2 In the case of networked personal computers the prime copy of all data must be held on the network file server(s).

6.8.3 In the case of stand-alone computers, users should be aware that disks are susceptible to failure and should hold a copy of all data files on backup media.

6.8.4 Arrangements must be made by the relevant departments in conjunction with the Head of Finance & ICT, for critical systems/operations to continue in the event of complete computing failure. This is addressed as part of the Council's Disaster Recovery & Business Continuity arrangements.

6.8.5 Back up copies of Corporate data, applications and documentation which is the responsibility of ICT will be stored away from the system to which they relate either in a restricted access, fireproof location or off-site (third-party storage, banks, neighbouring offices). Back up copies are regularly tested to ensure that they enable the system/relevant file to be reloaded in an emergency.

6.8.6 Back up copies of departmental specific data, applications and documentation should be stored away from the system to which they relate either in a restricted access, fireproof location or off-site (third-party storage, banks, neighbouring offices).

6.8.7 Back up copies should be clearly marked as to what they are and when they were taken. Depending upon the system concerned they should provide for system recovery at various different points in time over a period of several weeks. Backup media (disks, tapes etc.) do not last indefinitely, and should be periodically replaced with new media. ICT can offer advice in this regard.

6.8.8 Additionally, in certain circumstances, departments should make provision for the safe storage and retention of important records, (for example ledgers, vouchers, invoices/statements of account). Further information and guidelines on this issue can be obtained from Internal Audit in accordance with the laid down procedures.

6.8.9 You are directed to the provisions contained in **ISP 2.1 – Computer Backup and Recovery** for more specific information regarding the recovery of data from computer systems.

6.9 The Internet and the World Wide Web

6.9.1 Software for browsing the Internet such as Internet Explorer is provided to authorised employees and other agents for business use. Any personal use will only be allowed via the express permission of the Director or Head of Department. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be

associated with any for-profit outside business activity, and must not potentially embarrass the Council.

6.9.2 Any files downloaded over the WWW shall be scanned for viruses, using approved virus detection software provided by ICT as part of the Council's anti-virus procedures.

6.9.3 The use of WDC Internet connections for personal use during working hours is not permitted, unless prior consent is obtained from management, and is subject to the express condition that WDC is entitled to monitor such personal use.

6.9.4 Internet users are expressly prohibited from accessing, transmitting or downloading material that is obscene, pornographic, threatening, or racially or sexually harassing. No sites known to contain offensive material may be visited.

6.9.5 A Council-wide list of forbidden sites will be maintained. WWW software will be configured so that those sites cannot be accessed via corporate browsers. URLs (Internet Addresses) of offensive sites must be forwarded to the ICT Service Desk, to add to the maintained list of blocked sites. Internet sites containing offensive material will be immediately blocked by ICT network administrators.

6.9.6 Users of the WWW are reminded that web browsers leave "footprints" providing a trail of all site visits. Users are also reminded that all website activity is loged and retained.

6.9.7 Any user suspected of misuse may have all transactions and material logged for further action.

6.9.8 Any suspected misuse may result in investigation by Internal Audit and disciplinary action may follow.

6.9.9 All networked WEB browsers shall be configured to use the Council's firewall filters.

6.9.10 Requests for access to files or documents that are hosted by external vendors and which are larger than the councils size limits allow should be directed to the ICT Service Desk for guidance in the first instance.

Or

6.9.11 If any user has a requirement to retrieve files from online storage servers that are hosted by external parties, they should contact the ICT service desk with all relevant details and ICT will access the website, download the relevant file(s), virus scan them and pass on to the appropriate personnel.

6.10 Electronic Mail

6.10.1 Use of electronic mail (Email) for purposes which clearly conflict the Council's interests or are in violation of Council information security policies is expressly prohibited.

6.10.2 The Council provides electronic mail to authorised employees and other agents for business purposes. The use of WDC e-mail connections for personal use during or outwith working hours is not permitted, unless prior consent is obtained from management, and is subject to the express condition that WDC is entitled to monitor such

personal use The same rules apply as to what is regarded as inappropriate use whether during or outwith working hours.

6.10.3 Email address directories can be made available for public access within the provisions of the Data Protection Act.

6.10.4 The contents of email messages will be considered confidential, unless;

- In the case of investigations authorised by the Council's Chief Executive or nominated officer, and/or
- In circumstances where business critical or operational information is required, these requests must be authorised by senior management

6.10.5 Email communication will be retained by the Council for a minimum of 3 years plus current years. This will include deleted emails from both the sender and the recipient

6.10.6 Employees and other agents found to be deliberately misusing email will be disciplined appropriately.

6.10.7 Users must not allow anyone else to send email using their accounts Unless they have ***send on behalf of*** permissions set. ICT & Business Development can provide advice on how to setup this facility.

6.10.8 The Council reserves the right to review all employee and other agents email communications. Email messages may be retrieved by the Council even though they have been deleted by the sender and the recipient. Such messages may be used in disciplinary actions.

6.10.9 Incoming messages will be scanned by software for viruses and other malignant content.

6.10.10 If confidential or proprietary information must be sent via email it must be password protected, a freeware software application such as Winzip should be used, . Advice must be sought from ICT.

6.11 Acquisition and Disposal of ICT

6.11.1 All acquisitions should be in accordance with the provisions of the Council's Standing Orders and its Financial Regulations. Any queries should be directed to Corporate Procurement and/or ICT Service Desk.

6.11.2 The disposal or permanent hand-over of equipment, media or output containing personal or sensitive data must be arranged to ensure proper removal of confidential data.

6.11.3 Prior to the disposal of any PCs, ICT should be consulted to arrange for inventory details to be recorded and removed from inventory list. ICT will also advise if the permanent removal of all data and software programs is required or if the software can be transferred to another PC.

6.11.4 Disposals should be in accordance with the provisions of the Council's Standing Inventory Instructions. Disposals will normally be conducted by departments after

inspection of equipment by ICT. Instruction on the arrangements for the disposal of obsolete equipment must be co-ordinated through ICT.

6.12 Suspected Security Incidents

6.12.1 It is the responsibility of all members of staff to report any suspected irregularities/ fraud to their Director, or nominated senior officer, thereafter the Head of Audit, Performance & Strategic Planning as soon as possible, in accordance with the Council's Defalcation Procedures.

6.13.1 Information Security Education and Training

6.13.1 All Users will be provided with a pamphlet covering the basic aspects of Information Security.

7. Violations

7.1 Violations of this ICT security policy may include, but are not limited to, any act that:

- Exposes the Council to actual or potential monetary loss through the compromise of ICT security;
- Involves the disclosure of confidential information or the unauthorised use of corporate data;
- Involves the use of data for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body.

7.2 Any individual who has knowledge of a violation of this ICT security Policy must report that violation immediately to their Director or to the Head of Finance and ICT or to the Head of Audit, Performance & Strategic Planning. All further reports if required should be in accordance with the Council's Defalcation Procedures.

8. Disciplinary Process

8.1 Computer security is viewed seriously by the Council and any breach of this policy could lead to disciplinary action being taken against those who commit this breach. Violations such as the use of unauthorised software, the use of data for illicit purposes or the copying of software which breaches copyright agreements may be considered gross misconduct.

APPENDIX

Information on-

Copyright, Designs and Patents Act 1988
Data Protection Act 1998
Computer Misuse Act 1990

Copyright, Designs and Patents Act

Computer Users must not breach the legislation embodied in the Copyright, Designs and Patents Act (1988), which applies in particular to proprietary software and data, which must not be copied without the express permission of the copyright holders, except for the clearlydefined purpose of contingency (e.g. backups). Where required, any copyright notices should be included with any information provided by the Council to third parties.

The Data Protection Act 1998

The Data Protection Act requires that all computer processing of data relating to living individuals i.e. personal data, are registered with the Crown appointed Data Protection Registrar. There are a number of offences which, if the provisions of the Act are not complied with, will affect the Council, its employees and other agents. The Council has a series of registrations administered by Head of Finance and ICT who can give advice and answer queries on registration. The general provisions of the Act are:

- All processing of computer personal data must be registered;
- Personal data must only be processed as specified in the registration;
- Computer personal data must not be disclosed to any unauthorised person;
- On request, individuals have a right to a written copy of the data held; and
- Appropriate security measures must be taken to protect computer personal data.

The Computer Misuse Act 1990

Computer Users shall not, by any wilful or deliberate act, jeopardise the integrity of the computing equipment, its systems programs or any other stored information to which they have access. Under the terms of the Computer Misuse Act (1990), unauthorised access to a computer (sometimes called "hacking") or unauthorised modification to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences punishable by unlimited fines and up to 5 years imprisonment.

From 1st September 1990, three new offences were created under the above Act:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences; and
- Unauthorised modification of computer material.

In the first category, a person is guilty of an offence if he/she causes a computer to perform any function with intent to secure access to any program or data held in any computer AND the access or intended access is unauthorised AND he/she knows at the time when he/she causes the computer to perform that function that this is the case.

One should note that anyone using another person's user login and password, whether registered or not, will commit an offence at least under the first category. This applies equally to

accesses to and from any other computer, whether in this country or abroad. The copying of any data not specifically authorised, even into ones own files is an offence in the third category above.

Digital Economy Act 2010

The Digital Economy Act 2010 (c. 24)[1][2][3] is a law enacted by the Parliament of the United Kingdom regulating digital media. It received the Royal Assent on April 12, 2010, and entered into force on June 12, 2010.

The Act includes provisions about:

- the online infringement of copyright, including copyright and music companies' rights and about penalties for infringement
- the functions of Ofcom
- Internet domain registries
- the functions of the Channel Four Television Corporation
- the regulation of television and radio services
- the regulation of the use of the electromagnetic spectrum
- the Video Recordings Act 1984
- public lending right in relation to electronic publications
- amendment of the Communications Act 2003 requiring Internet service providers (ISPs) to disclose details of customers who repeatedly infringe copyright, on production of sufficient evidence, with a possible fine of £250,000 for non-compliance
- the requirement that ISPs block access to sites that allow "substantial" infringement