Personal Information Security Policy

Version 4.0
Policy Date: 13/06/14
Customer Relations & Information Governance Service
Business Strategy & Support

If you require further help in the interpretation of this policy you can contact the Corporate Information Governance Manager at keepdevonsdatasafe@devon.gov.uk

If this document has been printed please note that it may not be the most up-to-date version. For current guidance please refer to The Source.

This policy can be made available to the public, upon request, under the Freedom of Information Act 2000.

CONTENTS

1.0 Introduction

1.1 The purpose of this policy is to assist in the protection of all information assets owned and used by Devon County Council from the risks posed by inappropriate use. This includes protecting equipment and information from unauthorised or unlawful access, accidental or deliberate loss, damage, theft, disclosure or destruction.

1.2 It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy and keep our equipment and information secure. Agency workers and sub-contractors who are required to use the Council's systems, or undertake work in an area that contains personal data must also be made aware of, and will be expected to comply with this policy.

1.3 This policy explains what our expectations are when our computer equipment is used and our information is accessed. It must be read in conjunction with Devon County Council's Data Protection Policy. Further information about how to keep information safe, can be found on the Keep Devon's Data Safe website on the Source.

1.4 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the Data Protection Act 1998. All incidents will be investigated and action may be taken under the Council's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken.

2.0 Using our equipment

2.1 When using our equipment, the following rules apply:

2.2 A certain amount of limited and responsible personal use of our equipment is permitted.

2.3 No equipment, systems or information are to be used for your own commercial/business use or for political purposes.

2.4 Compliance with this policy is part of your employment contract. If you do not follow these rules and procedures, your use of the facilities may be withdrawn and disciplinary action may follow. In the most serious cases, this could be dismissal without prior warning.

2.5 All users must be made aware that Devon County Council electronically audits computers. In addition, sample random audits may be carried out.

2.6 All information relating to our customers and business operations is confidential. You must treat paper-based and electronic information with equal care.

2.7 You must have no expectation of privacy in your use of any Devon County Council business system. You must be aware that any correspondence, documents, records or handwritten notes you create for work related purposes, may be disclosable to the public, under the Freedom of Information Act 2000 or the Data Protection Act 1998. Any comments recorded or notes written must therefore be professional.

2.8 Further information about using our ICT equipment can be found in the Private Use of ICT Policy, available on the Source.

3.0 Internet Use

3.1 The Council encourages business use of the DCC website and the wider internet to help us improve our efficiency, effectiveness and management of information. The Internet must be used for lawful purposes only and you must comply with relevant legislation.

3.2 Internet access for personal use is at Devon County Council's discretion and must not be assumed as a given. Any misuse of this facility can result in it being withdrawn. Limited personal use of the Internet is permitted outside of normal working hours.

3.3 The Internet Use Policy, available on the Source, must be adhered to by anyone who uses the Internet, either for work or personal use.

4.0 E-mail Use

4.1 All employees, Members, contractors, agents and anyone else using a Devon County Council e-mail account must comply with Devon County Council's E-mail Policy available on the Source.

4.2 Sending information externally by e-mail is not always secure. E-mails can be intercepted and viewed by those who are not authorised to see it (e.g. 'hackers'). Therefore, personal or sensitive business information must not be sent to an e-mail address outside of Devon County Council, unless it is absolutely necessary and the transmission is secure for example, you **and**

the recipient have a secure e-mail account such as Government Connect and the appropriate protective marking is used. More information about how to transfer information securely can be found on the Keep Devon's Data Safe website on the Source.

4.3 If you cannot use a secure e-mail account and must share the information electronically, encrypt the document before you e-mail it. Do not put the password in the same e-mail. Send the password in a separate e-mail or give the person receiving the information, the password over the telephone. More information about how to send information securely can be found on the Keep Devon's Data Safe website on the Source.

4.4 An alternative way of transferring large amounts of data outside of Devon County Council, is by Secure File Transfer Protocol (SFTP). For more information, read Devon County Council's Encryption Policy available on the Source or contact your IT Liaison Officer.

4.5 If you receive an e-mail which is intended for another person you must notify the sender immediately and delete it from your Inbox. You must not make use of the information or disclose the contents of the e-mail to anyone else.

4.6 Microsoft Outlook has a facility called AutoPreview. This allows you to view the contents of an e-mail in the same window as your list of messages. It is recommended that this feature is switched off as there is a possibility that it could lead to a virus or other program contained within the body of the email automatically being run on the machine and therefore compromise security. With the AutoPreview feature being switched off you are able to review your emails so that the odd, or suspicious ones can be investigated further with out viewing the contents. This also allows you to read your email without being overlooked.

4.7 To turn AutoPreview off, click 'View' on your Inbox menu tool bar and click 'AutoPreview'. If you have 'Preview Pane' on instead, you must also turn this off so the contents of your e-mail cannot be overlooked. To turn this off, click 'View' on your Inbox menu tool bar and click 'Preview Pane'.

4.8 You must not attach anything to your e-mails which may contain a virus. You must take particular care with attachments from third parties as these might carry viruses and/or breach copyright rules. If you suspect you have received an e-mail containing a virus you must immediately contact the ICT Help Desk on 01392 38(2222). Do not forward the suspected e-mail to anyone.

5.0 Accessing and Monitoring E-mails

5.1 Devon County Council reserves the right to monitor e-mails, to ensure compliance both with the law and with Devon County Council's policies. Any monitoring carried out will be in accordance with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

5.2 There may be occasions when managers or other colleagues need to access or monitor your Inbox. For example, if you are off sick or are on annual leave. This is to ensure that any work related enquiries, sent to your work e-mail address, are dealt with in your absence.

5.3 Any e-mails sent to you which are clearly of a private and personal nature, must not be opened. However, where possible, you must have sensitive personal communications **about you**, sent to your home, to avoid accidental viewing.

5.4 You must not access or try to access another user's e-mail account, unless you are authorised to do so, or impersonate another person.

6.0 Telecommunications

6.1 All use of phones must be in accordance with the Telephone and Faxes Policy and the Mobile Phone Policy available on the Source.

6.2 Details of calls made (e.g. sent to/from, date, duration and cost) are recorded on all mobile and most fixed line telephones. It will be assumed that all telephone calls or Short Message Service (SMS) messages made or received on Devon County Council equipment, are for business purposes unless the contrary is indicated.

6.3 It is everyone's responsibility to ensure the safekeeping of any telecommunications equipment in their control. Any theft or loss must be reported to your Line Manager and the Information Governance Manager by completing the Security Incident Reporting Form.

7.0 Access to systems

7.1 It is a criminal offence under the Computer Misuse Act 1990, to deliberately attempt to access a system which you have no authority to access. ICT Services reserves the right to regularly monitor systems and unauthorised attempts at accessing systems may be investigated.

7.2 It is also a criminal offence under the Data Protection Act 1998 for any person to knowingly or recklessly; obtain, disclose, sell or offer to sell personal information, without the permission of the data controller (Devon County Council). This is subject to certain exemptions. Full details about this offence can be found under Section 55 of the Data Protection Act 1998.

7.3 Information created or collected as part of working for Devon County Council, is the property of the Council. Work related information must not normally be saved to an individual's M-Drive, for example 'My Documents' as a long term storage facility. Although the M-Drive is a secure place to hold sensitive information, it is only accessible to the desktop user so it is not appropriate to save business data such as information about clients, to this drive, as it prevents other team members who need to see it, from having access. Further information about where to save documents, can be found on the Records Management pages on the Source.

7.4 If work related information is held on a person's M-Drive, and that person is on annual leave or sick leave, a manager may request and be given access to this information. The M-Drive is the property of Devon County Council. There must be no expectation of personal privacy on this Drive. Personal photographs and videos must not be held on the M-Drive.

7.5 Members of the public and employees are entitled to see what information is held about them by Devon County Council. This includes handwritten notes, e-mails and any other information held electronically or in paper form. Personal information held on the M-Drive is also subject to the Data Protection Act 1998 and may be disclosable to the person who the information is about, if they make a request to see it. This is known as a Subject Access request. More information about this can be found on the Data Protection pages on the Source.

8.0 Passwords

8.1 All computer users are given a Username and Password; these are unique and must not be shared with anyone else. All passwords must conform to the Password Policy, available on the Source.

8.2 Passwords must not be written down, or kept where others might find them. Passwords must be hard to guess and must contain at least eight characters. They must include a mixture of upper and lower case letters, numbers and special characters such as ! # £ $. This makes the password more secure.

9.0 Security of equipment and information

9.1 Computer equipment that is logged on and left unattended can present a tempting target for unscrupulous staff or third parties on the premises. Unsecured laptops and other portable equipment must never be left unattended. They must not be left on view in vehicles, public transport or hotels or left unsecured on desks overnight, or left in vehicles overnight.

9.2 Users are required to screen-lock their computers when leaving the room, **for any length of time**. If an unscrupulous character has access to your computer, they can do a lot of damage, even in just two minutes. To lock your computer screen, hold down the keys Ctrl, Alt, Delete at the same time. The default must then be 'Lock Workstation' and can be set by pressing the return key. Using the 3 keys again when access is required and entering the password, restores the screen to its previous position and does not lose any data.

9.3 If your computer equipment cannot or does not allow a password protected screen-lock, you must inform the ICT Help Desk on 01392 38(2222).

9.4 All personal and sensitive business information held in any form e.g. on paper, CDs, memory sticks etc, must be locked away when unattended and not left on desks. This is to ensure that accidental or inappropriate viewing does not take place by those who are not authorised to have access to the information. Any confidential notes made during the day, must be securely stored or destroyed prior to leaving the office.

9.5 All confidential or sensitive information held in paper form, must be shredded or ripped up and placed in the pink 'confidential waste sacks', when they are no longer required. Personal or sensitive information must not be disposed of in the black general waste sacks. These sacks are not held or disposed of securely and can be accessible to the public.

9.6 All confidential documents that have been sent to a shared printer must be collected immediately, to ensure they are not picked up or read accidentally or deliberately by someone not authorised to see the information.

9.7 Some sites or offices may have a higher level of restricted access, for example via swipe card or number code. Part of this reason may be the security of information held on the premises. Staff and visitors are to abide by any rules when visiting or working in such sites.

10.0 Working Remotely

10.1 If you work remotely, you must adhere to the Mobile and Flexible Working Policy, available on the Source.

10.2 Working remotely can pose several security risks. To help reduce these risks, you must ensure you carry out the following:

- All remote working must be done using a Devon County Council managed Device (that is a PC, laptop, Blackberry or other mobile device supplied by The Council).

- Position yourself so that your work cannot be overlooked by others not authorised to see the information.

- Take precautions to safeguard the security of any computer equipment on which you do Devon County Council business, and keep your passwords secret.

- Inform the Police and the Information Governance Manager as soon as possible if any sensitive paperwork or computer equipment has been stolen or lost and complete the Security Incident Reporting Form.

- Ensure that any work you do remotely is saved on Devon County Council's system or is transferred to it as soon as possible.

- Ensure that secure ID tags or memory sticks are kept separately from computer equipment when not in use.

- Remember that these rules apply equally when you working at home. Not even a member of your family must have access to Devon County Council's information.

11.0 Information Security Incidents

11.1 The Council has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that Devon County Council can learn from its mistakes and prevent losses re-occurring.

11.2 The Council has developed and implemented an Information Security Incident Reporting Policy, you must ensure that you read and understand both the policy and your responsibilities under the reporting process. In all cases you must complete the Security Incident Reporting Form.

11.3 The Council also needs to take action where potential incidents are identified. Where 'near misses' occur, these must be reported to your line manager and a local decision taken as to whether the cause of the 'near miss' is one which could involve the enhancement of the policy or the process. If this is the case the Security Incident Reporting Form must be completed.

12.0 Disclosure of Information

12.1 Personal or sensitive business information held by Devon County Council must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information. Verification can be sought from the Information Governance Team when this is not clear. To learn more about sharing information, go to the Keep Devon's Data Safe website, available on the Source.

12.2 If you have received a request for information from a member of the public, or another organisation and they mention the Freedom of Information Act 2000 or the Data Protection Act 1998, contact the Information Governance Team on 01392 38(3445) as soon as possible.

12.3 All individuals disclosing personal, sensitive or confidential information by post, fax, email or telephone must read and comply with the Council's specific guidance relating to this, available on the Keep Devon's Data Safe web pages on the Source.

13.0 Social Media and Online Participation

13.1 Devon County Council has a policy on Social Media and Online Participation, available on the Source, which sets out the standards of behaviour expected when participating on online discussions, forums, blogs, websites and so on. You are not permitted to disclose personal information about Devon County Council's staff or clients or sensitive business information online, unless you are specifically authorised to do so by your manager and the recipients of the information are legally entitled to see the information.

14.0 Network Security

14.1 All Devon County Council computers have approved anti-virus software installed and this is scheduled to run at regular intervals. If you suspect your computer is infected with a virus, contact the ICT Helpdesk on 01392 38(2222).

14.2 Users must never download files from unknown or suspicious sources. All spam e-mails must be deleted and suspicious attachments or those from an unknown source must not be opened.

14.3 Users must never attempt to disable their anti-virus software on their computer. If problems arise, the user must contact the ICT Help Desk for assistance.

14.4 Any attempts by an employee to create and/or distribute malicious programs into the Devon County Council network (such as viruses, email-bombs, worms, network monitoring or 'sniffing' software, Trojans etc) are prohibited. Any user who engages in such activity will be subject to disciplinary and/or legal action.

14.5 ICT Services cannot control anti-virus systems on third party computers. Employees are to ensure that consultants and contractors do not plug their computers onto our network without prior approval from ICT.

15.0 Disposal of information and computer equipment

15.1 All personal or sensitive business information held in paper form must be destroyed securely when it is no longer needed. Devon County Council provides 'pink confidential waste sacks' for the disposal of this kind of information. In County Hall, these bags can be obtained and collected from Central Dispatch. Contact them direct on 01392 38(2505).

15.2 Alternatively, personal or sensitive information must be shredded, using a good quality 'cross' shredder.

15.3 If you have any redundant, faulty or unused hardware or software, contact the ICT Helpdesk on 01392 38(2222). Do not dispose of this yourself.

Policy Declaration

I confirm that I have read, understood and will adhere to Devon County Council's Personal Information Security Policy.

Signed: ……...

Printed: ……...

Line Manager Name: ……...

Directorate: ……

Service / Unit: ……

Date: ……...

To be returned to the HROne Admin Team

Policy History

Policy Date	Summary of Change	Contact	Implementation Date
Jan 2010	Insertion of Policy Declaration	A. Steer-Frost, Corporate Information Governance Manager	23 March 2010
Oct 2012	Insertion of paragraph 12.3	A. Steer-Frost, Corporate Information Governance Manager	17 October 2012
June 2014	Addition of 'network scanning software' in 14.4 Addition of 'Managed Device' bullet point in 10.2	A. Steer-Frost, Corporate Information Governance Manager	13/06/2014