Corporate Information Governance User Handbook

April 2010

This Handbook is intended to provide general summary information only and should not be taken as a full statement of the law or of the Council's policies and rules. If there is a difference between the Guide and the law then the law applies. Any difference between the Guide and the Council's policies and rules then the policies and rules apply.

1.0 Introduction

1.1 Information Governance

"*Information governance is a framework for handling personal information in a confidential and secure manner, to appropriate ethical and quality standards, in a modern local authority*".

Information governance sits alongside research governance and corporate governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal information. It provides a consistent way for staff to deal with the many different information-handling requirements, initially including:

- Information governance management
- Confidentiality and data protection assurance
- Information security assurance
- Corporate information assurance.

All staff need to learn about information governance to help ensure that they follow the best practice guidelines on information handling to enable them to manage personal information for the benefit of the public. The public will know that their records will not be disclosed inappropriately.

How this guidance will help you

This user handbook gives you a brief introduction to information governance and summarises the key user procedures that have been developed to support the Council's information governance policies.

The aim of this booklet is to ensure that you are aware of your roles and responsibilities for information governance.

It is your responsibility to ensure that you read the associated procedures and guidelines, which are available on the Council's intranet site under the information governance pages.

Remember…
Everyone is responsible
For information governance

2.0 Information governance policy statement

Objective

The objective of information governance is to maximise the value of organisational assets by ensuring that data is:

- 🔒 Held securely and confidentially
- 🔒 Obtained fairly and lawfully
- 🔒 Recorded accurately and reliably
- 🔒 Used effectively and ethically
- 🔒 Shared and disclosed appropriately and lawfully

Policy

The purpose of the policy is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of the Council to ensure that:

- 🔒 Information will be protected against unauthorised access
- 🔒 Confidentiality of information will be assured
- 🔒 Integrity of information will be maintained
- 🔒 Information will be supported by the highest quality data
- 🔒 Regulatory and legislative requirements will be met
- 🔒 Business continuity plans will be produced, maintained and tested
- 🔒 Information security training will be available to all staff
- 🔒 All breaches of information security, actual or suspected will be reported and investigated.

The user procedures and guidelines produced to support the policy apply to the Council and all its staff, agency staff, seconded staff and contractors.

3.0 Information Governance key user procedures

3.1 Human Resources Security

DO ✓

- Be aware of your responsibilities for information security
- Remember that you have signed a confidentiality agreement within your contract of employment
- Be aware that unauthorised disclosure or misuse of personal data will be treated as a serious disciplinary offence
- Ensure that temporary staff and third party users sign a confidentiality agreement
- Be aware of information governance procedures and guidelines
- Ensure that you receive appropriate training to enable you to carry out your work efficiently
- Ensure that your training needs are assessed on a regular basis
- Know how to report security incidents
- Be aware that the Council has a formal disciplinary process for dealing with staff who violate Council policies and procedures.

DO NOT ✗

- Attempt to prove a suspected security weakness, as testing a weakness might be interpreted as potential misuse of the system.
- Allow third parties access to the organisation's hardware, without correct authorisation.
- *Ignore security incidents!*

3.2 Physical Security

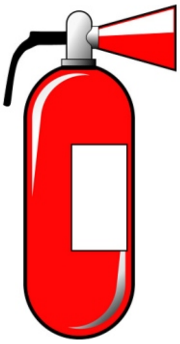
DO ✓

- Ensure all IT equipment is reasonably protected against theft and unauthorised access
- Follow the procedures for use of portable computer devices, mobile phones and removable media
- Ensure that assets are disposed of in accordance with the Council's procedures
- Wear ID badges
- Ensure that visitors sign a visitors' book and receive a visitors ID badge
- Challenge unidentified visitors in a controlled area
- Escort visitors in secure areas at all times
- Operate a clear desk and clear screen policy:
    - ♦ Confidential information should be locked away when not required
    - ♦ Incoming and outgoing mail points should be in secure areas
    - ♦ Confidential information should be cleared from printers and fax machines immediately
    - ♦ Password protected screensavers will be installed on all PCs (where possible)
    - ♦ PCs will not be left logged on and unattended - Ctrl-Alt-Delete, lock workstation
- Ensure keys to premises are securely stored
- Site computer screens away from unauthorised viewing
- Ensure that all deliveries are correctly checked, recorded and distributed in a secure manner

DO NOT ✗

- Take the Council's equipment, information or software off-site without authorisation
- Leave equipment unsecured in public areas
- Tell others what keys you have been entrusted with
- Disclose the codes for security keypad locks.

3.3 Environmental Security



DO ✓

- Be aware of the building fire procedures
- Know how to raise an alarm
- Recognise the sound of the fire alarm
- Know how to safely evacuate the building through two separate routes
- Know where the fire assembly points are
- Keep fire doors closed
- Maintain a neat and tidy environment and do not store anything that will burn next to a Source of heat (heaters, plugs, extension cables, electric sockets, IT equipment).
- Ensure that cabling does not trail and do not overload extension cables e.g. Running a double adaptor from a four-gang extension resulting in 5 appliances being plugged in.
- Ensure that cabling does not trail and the electric source is not overloaded
- Be vigilant when drinking around electrical equipment.

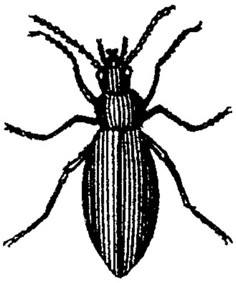
DO NOT ✗

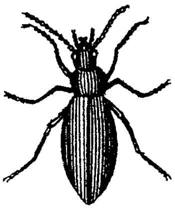
- Store inflammables near to any source of heat
- Site electrical equipment near to sources of water, e.g. pot plants, vase of flowers etc.
- Attempt to tackle an outbreak of fire unless you are trained or to facilitate an escape

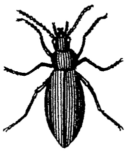
3.4 Protection against malicious software

DO ✓

- Ensure that anti-virus software is operating and is up to date
- Update virus checking software regularly on laptops
- Ensure that all files on electronic media of uncertain origin are virus checked before being loaded onto the network
- On discovering a virus:
  - Note any symptoms
  - Immediately shut down PC
  - Do not use infected media on another PC
  - Report it immediately to the IT Helpdesk
  - Ensure that all other possibly infected equipment is isolated
  - Use write-protected CD-Rom where possible







DO NOT ✗

- Remove or disable anti-virus software from a PC
- Change the way anti-virus software is configured
- Load unauthorised software including screensavers/games
- Use unauthorised software on the Council's equipment
- Attempt to "clear" an infected PC
- Open email with suspicious attachments; contact IT Helpdesk for guidance
- Accept any freeware advertised as it may contain spyware/adware, software used to gather Information about you and the organisation.

3.5 Data back-up, restore and file storage

DO ✓

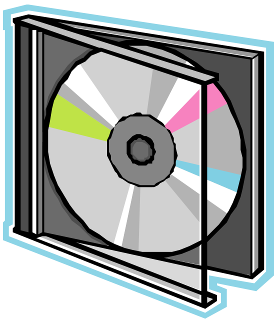
- Store confidential information on a shared area on the network - This will then get back up regularly and frequently by ICT Services
- Archive files and documents on a regular basis - delete documents you don't need anymore in line with the Retention Schedule Policy available in the Records Management Policy on the intranet

- Use removal
  (Including CD-Rom, USB memory sticks etc)

DO NOT ✗

- Misuse CD-Rom; exposure to heat will damage the surface and the data
- Store any information on your computer

If you do not have a shared area on the network to store information then raise a Work Request via IWantIT (available on the Intranet)

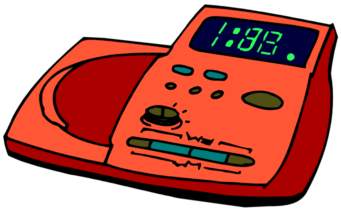


3.6 Exchanges of information and software

DO ✓

- Be aware of safe haven guidelines for confidential information, e.g. faxes
- Telephone the recipient and ask them to wait by the fax machine whilst you send the document
- Ask them to acknowledge receipt
- Check the number dialled, and check again before sending
- Where possible use pre-stored numbers
- Send a test fax first

- Take care when making a phone call to make sure that you do not reveal confidential information, e.g. by being overheard
- Take care when listening to answerphone messages, e.g. close the door when retrieving messages
- Be aware of the guidelines for confidentiality



DO NOT ✗

- Leave confidential messages on answering machines
- Leave confidential information on white boards
- Leave confidential information in message books
- Have confidential conversations in public places or open offices or meeting places with thin walls
- Disclose sensitive or personal information to anyone on the phone or via fax, unless you are sure they are who they say they are and that they need to know those details

3.7 Email security

DO ✓

- Be aware that the e-mail system is primarily used for business use. Occasional and reasonable personal use is permitted provided that it does not interfere with the performance of your duties and is in your own time.
- Be aware that the Council may inspect email addresses and contents (including personal e-mail) without notice
- Follow the email guidelines for e-mail etiquette and best practice, unacceptable use and retention of messages
- Be aware that the same laws apply to email as to any other written document
- Keep the number of email in your in box to a minimum
- Use an auto signature
- Be careful about content - email is easily forwarded
- Check your inbox regularly

- Use out of office assistance to advise people when you are not available
- When required, ensure email delegates are set up appropriately to allow access to your emails whilst out of the office, on holiday etc.
- Use the address book (or contacts) where possible, to prevent incorrect addressing
- Be aware that you do not own the documents that you or your colleagues create and you do not have intellectual property rights over them
- Report to IT any email that you receive, or become aware of that may be regarded as illegal or offensive
- Be aware that your mailbox may be opened to access information if absent, e.g. sickness or holiday
- Remove any personal contents from your mailbox and personal drive when leaving employment (it may be made available to a replacement or line manager)
- When sending an email, consider carefully who it needs to be sent to.

DO NOT ✗

- Leave email logged in and unattended
- Speak to the media, analysts or to the public on behalf of the Council via email unless you are duly authorised to do so
- Use an email to set up, maintain or promote personal business
- Send email that is or could be considered to be sexually or racially offensive, pornographic, defamatory, abusive, profane, could be construed as bullying, criminal or for any other unauthorised purpose
- Use email for commercial activities or to advertise goods
- Create or forward chain mail
- Send to large numbers of people unless you are sure it is directly relevant to their job - Spamming is not permitted.
- Send sensitive or personal data via a .gov.uk email address. Ensure it is sent securely via a .gcsx.gov.uk account (if you are unsure, contact the ICT Helpdesk)

3.8 Internet security

DO ✓

- Be aware that the internet and intranet is primarily for business use. Occasional and reasonable personal use is permitted provided that it does not interfere with the performance of your duties, and it is in your own time.
- Follow the guidelines for internet use
- Be aware the same laws apply to internet communications as for written documents
- Remember that the Council reserves the right to use monitoring and filtering software to prevent access to sites which are not work related or may have offensive or illegal content
- Remember that the Council reserves the right to undertake audits to monitor usage of the internet to ensure that it is not being used inappropriately
- Be aware that inappropriate use may result in prosecution and/or disciplinary action
- Be aware of spyware and adware software programs that surreptitiously monitor your actions. This software is used to invade your privacy gathering data about you and your organisation. Often bombarding systems with pop-up ads, causing countless problems to networks.

If you are offered something for nothing in an advert, you could be getting far more than you bargained for

DON'T CLICK

DO NOT ✗

- Leave the internet logged in and unattended you are responsible for what happens under your login
- View, download, transmit or archive any information, graphics, pictures, music, video clips that are contrued as bullying, defamatory, obscene, racist, sexual, or of a criminal nature
- Load executable programs or applications from the internet, this includes software and shareware
- Set up, maintain or promote personal business for commercial activities or to advertise goods or services
- Speak on behalf of the organisation in newsgroups or chat rooms
- Use the internet and web access in a manner that breaks any of the Council's policies

3.9 User access control - The system will lock your PC if left unattended for an amount of time. Best practice dictates that you remember to lock it when leaving the PC unattended.

DO ✓

- The network requires you to have an individual logon to access it. Ensure that any applications containing personal information that you use is accessed in a similar manner.

- Select quality passwords with a minimum of six characters which are:

  ♦ Easy to remember
  ♦ Not based on anything somebody else could easily guess, e.g. names, telephone numbers etc.
  ♦ A combination of letters and numbers
  ♦ Avoid re-using or recycling old passwords

- Keep passwords confidential - you are responsible for information entered using your password. Failure to protect your password or workstation could result in disciplinary action

- The network will require you to change your password at 90 day intervals. Ensure that you also change application passwords appropriately.

- If there is any indication of system compromise then please alert the ICT Helpdesk and change your password.

- Use password protected screensavers when away from your desk (activated by Control+Alt+Delete - lock workstation)

- Be aware that you are responsible for any activity performed under your logon ID and password. This includes any activity undertaken by someone else while your PC is left logged in and unattended without a password-protected screensaver.

- Ensure that you log off correctly i.e. don't just switch the machine off. Exit and shut down.

DO NOT ✗

- Leave a PC logged in and unattended

- Use someone else's ID or password

- Write a password down.

- Connect any unauthorised hardware to the Council's network, this will be considered a disciplinary offence

3.10 HomeWorking

DO ✓

- Obtain authorisation prior to working from home.
- Ensure that updated anti-virus software is used.
- Ensure that any Council equipment is used only by you, for authorised work only.
- Be aware that your legal duty to maintain confidentiality relates to data taken home.
- Ensure that a risk assessment is undertaken if you need to use confidential information at home.
- Follow procedures for the use of portable computer devices, mobile phones and removable media.
- Be aware that you use your own PC at your own risk. The Council will not be responsible for fixing faults etc.
- Be aware that you cannot connect your own PC to the Council network remotely
- Take regular data backups and ensure that they are stored and transported, securely.
- Be aware that it is your responsibility to ensure that you work in a suitable environment (health and safety). If in doubt, please speak to your health and safety advisor.
- Ensure that all confidential and sensitive data is removed from your PC before disposal or giving to someone else.

DO NOT ✗

- Email confidential or sensitive data to or from a home PC
- Connect your Council PC wirelessly to your router at home.

3.11 Compliance Requirements

DO ✓

- Be aware that the Council is obliged to abide by all relevant European Union legislation.
- Be aware of the following legislation:

- Data Protection Act 1998 (see DPA procedures).
- Freedom of Information Act 2000 (See FOI procedures).
- Access to Health Records Act 1990.
- Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990.
- Human Rights Act 1998.
- Follow the Caldicott principles. All health and social services departments must have a Coldicott Guardian, who must be a senior manager. The Caldicott Guardian makes sure that where confidential personal information is shared (eg with local NHS or other care partners), this is done properly, legally and ethically.
- Code of Connection
- Be aware that all staff are responsible for information security.

DO NOT ✗

- Breach legal requirements.
- Be ignorant of the legal requirements that affect you.
- Copy software illegally.
- Breach copyright laws.

3.11.1 Data Protection Act (DPA) Policy

The Council needs to collect personal information about people who it deals with so it can carry out its business and provide services.

Such people include clients, staff (present, past and prospective), suppliers and other business contacts. No matter how it is collected, recorded and used e.g. on a computer or on paper personal information must be dealt with properly to ensure compliance with the Data protection Act (DPA) 1998.

The lawful and proper treatment of personal information by the Council is extremely important. The success of our business and the confidence of our service users and staff is achieved by everyone knowing their roles and responsibilities. We ensure that the Council treats personal information lawfully and correctly.

The Council fully supports and complies with the eight principles of the Act.

Personal data must:

- Be processed fairly and lawfully.
- Be obtained or processed for specific lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be kept for longer than necessary
- Be processed in accordance with rights of data subjects.
- Be kept secure.
- Not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

All staff will:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand and comply with the eight DPA principles.
- On receipt of a subject access request from an individual for information held about them, immediately notify their line manager or the information governance team.

The Council will:

- Provide training for all staff who handle personal information.
- Carry out regular checks to monitor and assess processing of personal data to ensure the Council's DPA notification is kept up to date.
- Develop and maintain DPA procedures to include roles and responsibilities, notification, subject access, training and compliance testing.

THE COUNCIL'S DATA PROTECTION LEAD IS WITHIN THE RESOURCES DIRECTORATE

3.11.2 Freedom of Information Policy (FOI) Policy

The Freedom of Information Act (FOI) was passed in 2000 and replaces the Open Government Code of Practice that has been in place since 1994.The Act gives the public a general right of access to all types of recorded information held by public authorities.

The Act places a statutory obligation on all public bodies to publish details of all recorded information that they hold and to allow,with a few exceptions,the general public to have access to this information on request.

The Council recognises the importance of the Act and will ensure that appropriate systems are put in place to publicise what recorded information is kept by the Council and how this information can be accessed on request by the general public.The overall responsibility for this policy is with the Chief Executive.

All staff will,through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the storage, closure,retention and disposal of documents and records.
- Be aware that ultimately the general public may have access to any piece of information held within the Council and must pay due regard to how they record information as part of their normal duties.
- On receipt of an information request,immediately notify the FOI lead.
- Provide information promptly when requested by the FOI lead (the Council has only **20 working days** to respond to a request).

The Council will:

- Maintain and publish a publication scheme.
- Provide all staff with an introductory briefing on the FOI Act and related procedures.
- Develop and maintain clear procedures for recognising and responding to requests for information under FOI.
- Develop and maintain a comprehensive record management strategy that supports FOI.

The Council's FOI Lead is Paul Martin - Ext. 1066

**The Council's FOI Legal Advisor is: Rob Barnett,
Group Solicitor (Policy Regeneration) - Ext. 1052**

3.12 Software and data management

DO ✓

- Be aware that shareware, freeware and evaluation software is bound by the same policies and procedures as all software. Advice must be sought from the ICT Helpdesk if you require this type of software
- Be aware that the software policies apply to laptop and hand-held devices as well as desktops.
- Be aware that the Council forbids the use of any software that does not have a licence, and anyone found to be using, or in possession of, unlicensed software will be subject to disciplinary procedures
- Respect all computer software copyrights and adhere to the terms and conditions of any licence to which the Council is a party
- Store licenses, invoices and original media securely for software purchased locally
- Actively and frequently undertake housekeeping of your data

DO NOT ✗

- Install software without authorisation including freeware, shareware, trial software
- Install non-business software e.g. games, unless authorised to do so
- Copy software from the Council's systems onto your own PC, e.g. at home
- Store personal data on Council systems, e.g. photographs, music files, videos

Remember
All PCs are actively monitored and audited.
Any unauthorised software will be detected, and may result in disciplinary action.

3.13 Records Management Policy

DO ✓

🔒 Be aware of the Records Management Policy and procedures and ensure that you:

- know the retention times for records
- follow the corporate filing structure when creating records
- ensure records are disposed of appropriately
- know who your local records manager is
- be factual, consistent and accurate, e.g. ensure records are
- Ensure documents are written as soon as possible after an event has occurred
- written clearly, legibly and in such a way that they cannot be erased
- readable on any photocopies
- clear, unambiguous, and concise (where possible)
- written in terms that the service user can understand

🔒 Ensure manual records are:

- Formally booked out from their normal filing system
- Tracked if transferred, with a note made or sent to the filing location of the transfer
- Returned to the filing location as soon as possible
- Stored securely within the office, arranged so that the record can be found easily if needed urgently
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons
- Held in storage with clear labelling indicating sensitivity and permitted access

DO NOT ✗

- Use unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation or offensive subjective statements.
- Record personal opinions/comments.
- Leave sensitive or confidential information where it can be accessed inappropriately.

4.0 How to report an information security breach

A security breach, loss of data etc. is any event, which has resulted in, or could result in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the system of data being put at risk
- The availability of the system or data being put at risk
- An adverse impact, e.g.
- Threat to personal safety or privacy
    - Legal obligation or penalty
    - Financial loss
    - Disruption of activities.

All incidents, or information indicating a suspected incident, should be reported as soon as possible to your line manager.

If data is lost the Council would consider notifying the Information Commission of the loss and inform those people whose information has been lost.