Information Handling Practices

2018

DAVENTRY DISTRICT COUNCIL

Document control template

Organisation	*Daventry District Council*
Title	*Information Handling Practices*
Author	*Vikki Smith*
Filename	
Subject	*Information Governance*
Protective Marking	*Normal*
Review date	June 2020

Revision History

Version	**Revision Date**
1.0	*09/05/2006*
1.1	*07/06/2013*
1.2	*10/06/2015*
1.3	*13/06/2018*

Document Approvals

This document requires the following approvals:

Sponsor Approval	**Date**
Senior Management Team	2 October 2017

Document Distribution

Distributed to	**Date**
Council wide	June 2018

DAVENTRY DISTRICT COUNCIL

SECTION 1 INFORMATION HANDLING PRACTICES

1. Introduction

1.1 Purpose

2 Background

2.1 Why does the Council need to manage information?

2.2 What are the risks of not managing information?

3 Scope

3.1 What information do these practices apply to?

3.2 To whom do these practices apply?

3.3 Integration with other policies

4 What the Council will do

5 Roles and responsibilities

6 Training and awareness

7 Retention and review

8 Compliance audits

SECTION 2 RETENTION AND DISPOSAL SCHEDULE

1 Introduction

1.2 Purpose

2 Access to information

2.1 Access to information and Members

3 Protective markings/Classification

3.1 Roles and responsibilities

3.2 Information created outside of the Council

3.2 Email encryption

4 Transfer of custody and ownership of information

4.1 Guiding principles for overseeing change

5 Safe disposal of information

SECTION 3 – MANAGING ELECTRONIC INFORMATION

1. Introduction

2. New documents: creating and organising them

3. Retention and disposal

4. Controlled access to IT systems

Appendix A

Legislation, Standards and Best Practice

Appendix B

Retention and Disposal Schedule

Appendix C

Record keeping system

Appendix D

Disposal Register

Appendix E

Document control template

Section 1
Information Handling Practices

1. Introduction

1.1 Purpose
The Information Handling Practices aims to ensure that full and accurate records of all activities and decisions of Daventry District Council ('the Council') are created, managed, retained and disposed of appropriately, and in accordance with legal obligations and professional standards. Related legislation, standards and best practice can be found in Appendix A.

2. Background

2.1 Why does the Council need to manage information?
Maintaining appropriate and effective information management practices will help the Council to deliver and meet its statutory duties and support its vision.

By adopting these practices the Council aims to ensure that the information, whatever form it takes (electronic, paper, audio etc.) is accurate, reliable, ordered, useful, up to date and accessible whenever it is needed. This will enable the Council to:

- help deliver services to the public
- help to make informed decisions
- protect the rights of the public and safeguard employees
- track policy changes and development
- ensure compliance with relevant legislation
- provide an audit trail to meet business, regulatory and legal requirements
- ensure the Council works effectively as public authority
- support continuity and consistency in management and governance

2.2 What are the risks of not managing information?
The Council recognises that there are risks associated with non-compliance with the law. The practices outlined in this document aim to mitigate risks such as:

- Inappropriate disclosure of information, leading to major incidents
- Legislative or financial penalties
- Loss of reputation and damage to the Council's corporate image.

3. Scope

3.1 What information do these practices apply to?

This document encompasses all information created by the Council regardless of media type. This means it includes paper and electronic information, as well as items held in audio-visual formats. There is further guidance in Section 3 regarding the management of electronic information.

3.2 To whom do these practices apply?

The practices described apply to all employees of the Council (both permanent and temporary), Elected Members, contractors and consultants who have access to Council information.

3.3 Integration with other policies and practices

The overarching document for all information-related practices is the Information Risk Policy, with all other information-related policies, procedures and practices, sitting below.

Implementation of the Information Handling Practices will include consideration of its position under the Information Risk Policy and its impact upon and integration into other relevant Council policies and practices, including:

- ICT Usage Practices
- PSN Acceptable Usage Policy
- Employee Handbook – Code of Conduct for Employees
- Data Protection Policy and Manual
- Information Security Incident Management Policy and Procedure
- Social Media Protocol
- Guide to Information
- Business Continuity Plan

Compliance with the Information Handling Practices will in turn facilitate compliance not only with information-related legislation but also with other legislation or regulations (including audit, equal opportunities and the Council's Constitution) affecting the Council.

4. What the Council will do

To ensure compliance with all legislation and regulations concerning the proper management of information, the Council will:

- Ensure officers are supported in their work, by providing access to up-to-date Council policies, procedures and necessary precedent information.

- Ensure that information is kept securely and protected from accidental loss or destruction.

- Ensure systems and procedures are put into place so that:
  - Appropriate documents and artefacts are captured as records
  - Information can be easily accessed by those of appropriate authority
  - Information is properly titled, referenced, indexed and, where necessary, protectively marked.
  - Information is available for as long as it is required in accordance with legislation and disposed of appropriately when no longer required (See Appendix B for the Retention and Disposal Schedule)

- Ensure that officers and Members retain an audit trail of all information that has been destroyed

- Ensure that as systems evolve, attention will be given to preservation of existing information in line with the Retention Schedule, ensuring the contextual qualities of the information can be maintained for as long as the information is needed. This is particularly important for information held electronically.

- Ensure all officers and Members who create and use information receive appropriate guidance in order to comply with the Information Handling Practices guidance.

5. Roles and responsibilities

The Council will develop a culture that properly values, protects and uses information for the public good.

Responsibilities:

Senior Management Team

- Approving the guidance for the disciplined management of information
- Communicating the guidance to employees throughout the Authority

Resources Manager

- To act as Senior Information Risk Owner (SIRO), with overall responsibility for Information Management, and the Retention and Disposal Schedule within the Council. This is further supported by the Data Protection Officer and Information Officer.

Governance & HR Manager

- To act as Data Protection Officer, with overall responsibility for the processing and management of personal data
- Develop, implement and maintain the Council's Data Protection Policy and Manual
- Identify the Council's training needs and ensure appropriate delivery
- Identify, monitor and advise on information sharing and data processing agreements, ensuring that they deal with data in a manner consistent with the data protection principles
- Advise service managers of their responsibilities with regard to data retention and disposal
- investigate breaches of the legislation, provide recommendations and oversee their implementation
- Create 'best practice' guidance for data processors

Service Managers

- Ensuring compliance with Information Handling Practices guidance within their Service Area
- Ensuring officers manage data in accordance with the team's Retention and Disposal Schedule
- Ensure each team has in place a record keeping system (paper or electronic) that holds its records securely and provides for quick and easy retrieval of information. See appendix C for guidance on a Record Keeping System
- To act as Information Asset Owners (IAO) within their Service Area, with responsibility for understanding and addressing risks to the information assets they 'own'
- To determine employees level of access to information systems within their Service Area
- Regularly review access permissions to their systems.

Information Officer

- Advising teams on the retention, management and storage of information
- Day-to-day management and co-ordination of Retention and Disposal Schedules.

IT Service Manager

- Providing archival and storage facilities for electronic information
- Ensuring backup tapes are stored securely and disposed of after one year
- Provide guidance on IT security.

Facilities Management function

- Providing office and storage facilities for the appropriate storage of physical records, either current or archival
- Arranging facilities for the disposal of information when they are no longer needed
- Arranging transfer of time-expired information of heritage value to County Archives.

Officers, Elected Members, contractors/suppliers, agency staff, partners and third-parties

To understand and adhere to their responsibilities for managing Council information, in particular responsibilities include:

- Ensuring actions and decisions taken in the course of Council business are properly recorded
- Creating, receiving and retaining information in line with corporate policies and practices
- Classifying information created in accordance with agreed business-based classification scheme/privacy markings and/or naming standards agreed within Service Area
- Ensuring information is disposed of in accordance with the Retention and Disposal Schedules
- Using information responsibly, fully respecting protective and security markings and considering the rights of individuals
- Raising any issues of non-compliance with Senior Management, Service/Line Manager or Data Protection Officer.

6. Training and awareness

As all employees are involved in creating, maintaining and using information, it is vital that everyone understands their information management responsibilities.

All employees and Members (including contractors and temporary staff) will be expected to conform to the practices outlined in this document, in respect of information handled in their role. Managers will be expected to support their teams, provide training on operational matters and monitor employees' performance.

Training and guidance will be provided to ensure that all employees are aware of their obligations in relation to Data Protection and Information Handling.

7. Retention and review

The Information Handling Practices guidance will be reviewed every three years, or sooner, if there is a significant change. The Retention and Disposal Schedule is an active document that will change as required throughout the year. It will be validated by Service Managers each year.

8. Compliance Audits

The Data Protection Officer will undertake an assessment of the effectiveness of the practices identified within this document along with additional knowledge requirements and report annually to the Corporate Governance Committee. Training needs will be incorporated into the Council's corporate development programme.

Section 2
Retention and Disposal Schedule

1. Introduction

As a public body the Council is required by law to manage its information properly. Legislation such as and the Freedom of Information Act, Environmental Information Regulations and Data Protection set out specific requirements in relation to the creation and management of information.

A. The Code of Practice on the management of records, issued under section 46 of the Freedom of Information Act, sets out the fundamental requirements of having good information management in place.
B. The Data Protection principles set out the requirement to ensure information is accurate, relevant, and not excessive, is not kept for longer than is necessary and is secure.

Through adhering to the principles of good information management the Council will benefit from:

- records being easily and efficiently located, accessed and retrieved
- information being better protected and securely stored
- information being shared only with those with the 'need to know'
- records being disposed of safely and at the right time

1.2 Purpose

The purpose of the Retention and Disposal Schedule is to:

- Ensure that the Council uses all appropriate and necessary means to ensure compliance with retention and disposal legislation and best practice guidance

- Provide guidance on the management of records created as part of the policies, decisions, functions and/or other activities carried out by the Council. The schedule will help Service Areas to:
    - Identify records/information
    - Determine what information needs to be kept and where
    - Determine which protective markings need to be applied
    - Determine when information needs to be destroyed or archived

- Provide consistency for the destruction of information no longer required for legal, financial or administrative purposes

- Prevent information from being destroyed prematurely where there are legal, financial or administrative requirements affecting their retention

- Support the Council to meet its statutory requirements, in relation to Information Legislation (Freedom of Information, Data Protection etc.)

- Assist with identifying information with potential for permanent preservation

- Promote improved information handling practices

2. Access to information

The Council needs to ensure that decisions regarding access to information, particularly public access, are documented so that they are consistent, and can be explained and referred to. In particular, the Council needs to ensure that:

- All employees and Members are aware of the arrangements for allowing access to specific categories of information (see Section 2.1 for specific guidance relating to Members).
- Procedures are in place to document decisions concerning authorised and withheld access.

Under the Freedom of Information Act, there is increasingly a presumption that government information should be considered 'Open' (i.e. accessible to all) unless there is a specific legal or business reason for limiting access. The Retention and Disposal Schedule will identify those records that are 'Open', and those that are not, by specifying the protective marking. Material produced with the express intention of informing the public, and actual Council publications, are fully accessible and listed in the Council's Guide to Information.

2.1 Access to information and Members

Information produced or received by Councillors as elected members is ***not*** covered by the Freedom of Information Act (FOIA). Therefore, information received, created or held by an individual Member will be subject to the FOIA only if the Councillor is acting on behalf of the Council for example being a Committee Member. In summary:

1. Information is subject to the Freedom of Information Act if it is held by a public authority on its own behalf, or is held by someone else on behalf of the public authority.
2. Correspondence between Members, or information held by a Member for their own private or political purposes, will usually not be covered by the Freedom of Information Act.
3. Information received, created or held by a Member on behalf of the Council will be covered by the FOI Act, for example, where a Member is part of a Council committee.
4. Information created or received by a Member but held on the Council's computer system or premises will only be covered by the FOI Act if it is held for the Council's own business.
5. Personal information held by Members should be handled in line with the Data Protection Act 2018/General Data Protection Regulation (GDPR).

Members are not public authorities in their own right and therefore, they have no obligation to respond to a request for information addressed to them individually. However, as a matter of good practice, Members should explain this to the requester and, with the permission of the requester, pass on the request to the Information Officer to process on behalf of the Council.

3. Protective Markings

Employees who send personal or sensitive customer information to government organisations like the NHS, the Department for Work and Pensions, Criminal Justice Agencies and the Police etc. have access to a secure email on a network called PSN – Public Services Network. It enables secure data sharing across government. This is part of a pan-government programme called Government Connect.

The protective markings applied to PSN emails are shown below. These classifications should only be applied to information transferred by PSN.

All other Council information (paper and electronic) shared outside the PSN should refer 3.1 "Local Handling Arrangements"

3.1 Local Handling Arrangements

Information needs to be trusted and available to the right people at the right time. The failure to share and exploit information can impede effective Council business and can have severe consequences (e.g. for the safeguarding of vulnerable people). The principles of openness, transparency, Open Data and information reuse require individuals to consider the proactive publishing of public sector information and data sets. However, there must always be a reasoned judgement, taking data protection and confidentiality into account.

The local handling system is based on the "need to know" and is determined by the creator of the information. There are two tiers:
NORMAL
CONFIDENTIAL

There would be no requirement to explicitly mark routine NORMAL information (all emails are automatically marked as NORMAL). Only where the information meets the

"CONFIDENTIAL" criteria would the document/email/record need to be marked accordingly.
For example, information which could have more damaging consequences (for individuals or the Council generally) if it were lost, stolen or inappropriately disclosed will attract additional security measures to reinforce the "need to know". In such cases where there is a clear and justifiable requirement to reinforce the "need to know", records/assets (such as emails/reports/contracts etc.) should be explicitly marked: "CONFIDENTIAL". This lightens the burden of marking everything, all the time.

The CONFIDENTIAL mark should be used for the following categories of information. This would be determined by the creator of the information.

Category 1: personal data, which includes -

Personal data, such as the names of private individuals (not sole traders or company names); if not already public, national insurance or NHS numbers etc. Broadly speaking this means data from which a natural person/living individual can be identified and the data relates to that individual is classed as personal data. This will also include sensitive personal data, such as racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and criminal matters.

This does not include the names/contact details of business individuals for example solicitors, company directors, sole traders, unless specifically asked to keep confidentially.

Category 2: commercially sensitive data, which includes –

Commercially sensitive data is information that if disclosed would (or would be likely to) prejudice the commercial interests of any person (including the Council holding it). For example, financial models/costing information/pricing information, trade secrets, some procurement activities, competitive bids, financial and business viability data, credit checks, legal advice, etc. in relation to a third party or the Council.

In addition to complying with these requirements, where legal privilege is involved, ensure that the rules surrounding this are followed. Correspondence should be marked as legally privileged and circulation restricted to those who need to know.

See below examples of how NORMAL and CONFIDENTIAL is applied.

Information Marking		
Legal and statutory obligations, in particular the data protection principals, legal professional privilege, crown copyright etc. will be followed, whatever the protective marking used.		
	NORMAL	**CONFIDENTIAL**
General points	Be stored and managed securely within DDC approved systems Handled in line with local guidance on Handling Information and clear desk principles. Examples include unpublished reports and financial information etc.	Not be left unattended and should be locked away when not in use. Only communicated or passed to others on a need to know basis Examples as mentioned at 3.1 above, such as employee records, payroll data, sickness information, customer information, fraud cases, as well as commercial sensitive information such as commercially sensitive contracts, bids, legal advice, etc.

Emailing material	By default this information can be sent over the Internet. No restrictions on emailing information, however it should be limited on a 'need to know' basis. You may choose to include additional handling tag and/or instructions, if appropriate. When receiving email you must follow any handling guidance stipulated by the sender. Where necessary adopt the transmission technique as used by the sender (e.g., encryption of message if sending outside your email domain). Where information you have added has increased the sensitivity you may choose to encrypt to provide additional protection.	Permitted to known contacts on a 'need to know' basis. Emails should be flagged as CONFIDENTIAL by the drop down option in outlook, or use another secure email method (e.g. PSN or Egress). You must follow the document originator's lead on encryption when replying to or forwarding emails, but may increase the level of security if considered appropriate. Information should normally be sent by encrypted/secure e-mail outside of DDC (subject to the exception above). Encrypt emails by flagging as CONFIDENTIAL in the drop down option in outlook. Information can be sent unencrypted only after making a risk based decision on the likelihood of it being intercepted and the level of damage that may be caused.

<table>
<tr><td>Moving information (by hand or post)</td><td>BY HAND:

Authorisation should be obtained from the Information Asset Owner if moving a significant volume of assets / records / files.

BY POST/COURIER:
Envelope(s) or parcel.

MOVING ASSETS OVERSEAS (BY HAND / POST / COURIER):
Envelope(s) or parcel.</td><td>BY HAND:

Carry in a nondescript bag in order to not draw attention to the contents.

Never leave papers unattended unless secure.

BY POST/COURIER:
Include return address on back of the envelope.
Do not normally mark the classification on envelope.

Consider using registered Royal Mail service or other reputable commercial courier’s ‘track and trace’ service.

MOVING ASSETS OVERSEAS (BY HAND / POST / COURIER):
Either by:
Trusted hand under single cover;
or:
Include return address on back of the envelope.

Consider using registered Royal Mail service or other reputable commercial courier’s ‘track and trace’ service.</td></tr>
<tr><td rowspan="2">Faxing</td><td colspan="2">Faxes should not be assumed to be secure. Consider using encrypted email if possible to communicate sensitive information.</td></tr>
<tr><td>Confirm the recipient’s fax number.</td><td>Sensitive material to be faxed should be kept to an absolute minimum.
Recipients should be waiting to receive faxes containing personal data marked CONFIDENTIAL.</td></tr>
<tr><td>Printing</td><td colspan="2">Permitted – but print only what you need.</td></tr>
</table>

Photocopying	Permitted – but make only as many copies as you need, and control the circulation of sensitive material.	
Storage		
Physical storage (of documents, digital media, when not in use)	Protect in line with local guidance on Handling Information and clear desk principles. This may include: protecting physically within a secure building by a single lock (e.g. a locked filing cabinet, locked drawer or container); not leaving papers on desks or on top of cabinets overnight. Only encrypted laptops may be used.	
Electronic storage	Information classed as NORMAL will be available to all within the team.	Any electronic document received marked CONFIDENTIAL should be saved according to its sensitivity. Appropriate controls must be used to restrict access and shared only to those that need to know. For example, some Finance and HR folders are available to only a limited number of colleagues and therefore access is restricted to the folder by IT Services. Permission to view the files should be granted by the Information Asset Owner.
Electronic storage on digital media (USB memory sticks, CDs, DVDs)	Only DDC (IT Services) supplied and approved portable media is to be used. The media must be encrypted.	
Disposing of physical documents	Dispose of documents appropriately: Information already in the public domain can be disposed of by recycling or as ordinary waste. Information marked CONFIDENTIAL must be disposed of with care, either using a secure disposal bin or by shredding using an approved cross-cut shredder.	

Remote working	
General Points	Laptops, smartphones (DDC issued or BOYD) and removable media used to store CONFIDENTIAL information must be encrypted. ICT Usage Practices should be followed here, specifically: - no sensitive or classified data may be stored on the device i.e. outside of the MDM software & DME encryption. - or entered into any applications that reside solely on the smartphone such as email, calendar, contacts, notes etc. Business information must not be emailed to or from staff home/personal email accounts. Limit the amount of information you take out of the office. Only take what is necessary.
Telephoning, video/call conferencing and other tools	No restrictions but take care of how your discussion might be perceived by others in earshot. When discussing confidential information via call conferencing check who is in attendance at the recipient organisation to avoid confidential information being broadcast too widely.

3.1 Roles and Responsibilities

Originator. The originator of a document (or any other format of information) is responsible for setting the Protective Marking of that particular document/information (digital or paper) at the initial stage of document creation. Over time it might be necessary to change the protective marking of a document/information; this is also a responsibility of the originator.

Line managers/Information Asset Owners have the responsibility of ensuring that marking of sensitive information is done in accordance with the guidance provided. They have to keep in mind the availability of information for others and the impact involved with high protective marking.

User/keeper can challenge the applied protective marking. They can never change the marking that has been applied by the originator of the information unless they have the consent. All employees in possession of information with a protective marking are responsible for handling the information in accordance with this marking. This includes storing, processing, sharing and destroying.

3.2 Information created outside of the Council

Information that originates from outside of the Council may not be protectively marked. If it is received by the Council then the Council should consider marking the document on receipt in line with the Local Handling Procedures.

Information received by the Council which already has a protective marking should be respected and held and processed in line with that protective marking.

Information that is marked with a marking that is not recognised should be assessed and regard must be had to the sensitivity of the document. For example documents may be received that are marked "private". It is advisable that such documents should be assessed in accordance with the sensitivity of the information and considered whether it is information that is truly either private in nature. Consideration should be given whether such documents should be marked "**CONFIDENTIAL**" by default.

3.3 Email encryption

Daventry District Council has a responsibility to ensure that all potentially sensitive data sent from the organisation is secure in transit over the Internet.

To help meet this requirement the Council has introduced an email encryption system available to all employees and Councillors.

Sender and Recipient user guides are available from the HelpDesk section of Davnet.

4. Transfer of custody and ownership of information

Advance planning for the transfer of information is critical, as the consequences of getting this wrong can be far-reaching. Failure to transfer information and knowledge effectively between organisations can make it impossible to maintain business continuity.

If there is a change in ownership of the information, for example if the Council outsources a function, a decision must be made about who owns the existing information which documents that activity. An example of this is when the Council transferred its housing stock to a housing association.

The options include:

- ownership of the information will pass to the new owners
- ownership will be retained by the Council but custody of the records is transferred
- both the custody and ownership of the information is retained by the Council.

4.1 Guiding principles for overseeing change

The Senior Management Team should apply the following guiding principles in overseeing the change:

- Advance contingency planning will enable the change to be implemented swiftly.
- The process must be jointly owned and managed by both organisations.
- Both should approach the change in a spirit of openness and co-operation.
- The outcome must enable both bodies to comply fully with legislative requirements e.g. Freedom of Information.
- There must be a focus on effective communication with the end-user or customer e.g. to meet the Data Protection principles.
- Opportunities for realising savings and efficiencies or managing records in innovative ways must be seized.
- Adequate resources must be made available to ensure business continuity, especially in high-profile and customer-facing areas.

Any change in ownership of information needs to be documented in the appropriate Retention and Disposal Schedule.

There is specific guidance on the transfer of knowledge, information and records from the National Archives http://www.nationalarchives.gov.uk/.

5. Safe disposal of information

Information that has been identified for disposal must be destroyed in a way which reflects its security status, sensitivity or confidentiality.

The Council is required to record what information has been destroyed, when it was destroyed and on whose authority. This is to ensure that the Council can show that information is destroyed on a systematic and routine basis e.g. when a Freedom of Information request covers information which has been destroyed.

Where records are disposed of to an outside agency (such as a confidential waste operator or a waste paper merchant) a certificate of destruction should be produced by the company concerned to indicate that the information has been pulped.

All information must be disposed of in a way which complies with the Council's information security policies and in line with the Council's environmental policy. Disposal methods are identified in the Retention and Disposal Schedule. The Disposal Register should be completed for all records destroyed.

Once hardware has been decommissioned and it has been decided that it is not suitable to be refurbished it must be recycled in accordance with the Waste Electrical Electronic Equipment (WEEE) Directive.

Section 3
Managing Electronic Information

1. Introduction

This section provides practical guidance for managing electronic information, such as creating, organising, disposal and controlling access.

The essential truth about electronic records is that like weeds in the garden they will keep on growing and getting out of control unless you take measures to manage them on a pro-active basis. This section of the guidance will help you to manage the information you hold.

2. New documents: creating and organising them

You are just about to start drafting a new document, and you may be wondering how it is going to fit in with all the other items you have on your computer. Here are some pointers for carefully negotiating the first stage in the information management process. Some of them may not apply if you are using pre-defined templates or forms.

(a) Creation of the document

There are some features which every document needs, to enable you or others to identify it, place it in its proper context, work out its significance and decide whether it is up to date.

These are:-

- A title or name, both for the document itself and its reference within the Microsoft folder system
- A specific place within your folder system
- A version number, if it is an item which will be revised
- A reference to when it was created

Some questions to ask yourself:-

- Does the title clearly describe the subject matter?
- Does the title possibly duplicate some other document?
- Is the document a 'one-off', or is it a draft which may need to have different versions before it is approved and used?
- Is this a 'record', i.e. part of an established record series listed in the official Retention and Disposal Schedules? Or is it part of some supporting documentation or a working document for temporary purposes?
- Have you got a carefully planned folder system which accurately organises your material, and do you know where your new document should be placed in the system?

Some of these questions apply equally to email as they do to your Word, Excel or PowerPoint documents. You should find an answer to all of them before you finish working on your item.

Three vital things to remember:

1. DO NOT use your C:\ drive or desktop to store official documents: if you have to work on your C:\ drive temporarily, remember to transfer it onto the shared network drive as soon as possible.
2. DO NOT leave official documents on your personal drive. Only use this for drafts and rough working.
3. Information and documents on the C:\ drive will be lost if your hard drive fails or if you leave the organisation.

(b) Title or name
This should not be longer than seven words, but should reflect the contents and context. If you are skimming through your folders and cannot remember what a particular document refers to, then you may need to rename or review it.
Code words, or titles which do not properly describe the contents, are not a good idea, either for individual documents or folders. Reference numbers, as short as possible, can be used, but only where there is a specific purpose to them.

For the purposes of the file description for the folder, check the title before you complete the process. This should be no longer than four words. Avoid the use of underscores where at all possible.

If you have to include a date or date range in the folder file name, use the conventions YYYYMMDD, YYYYMM, or YYYY – YYYY, so that if these are listed in your folder the sequence will make sense.

When including a name, e.g. a service user, which will appear as one of a long list in your folder, use the surname followed by initials for the purposes of the folder.

Avoid using generic words as the first element of the file name: e.g. 'Draft Agenda' is wrong, but 'Agenda (draft)' is better. This helps with putting your documents in proper alphabetical order within the various folders.

(c) Document status
If the document is a draft, then include the word Draft in the Header section and a version number in the Footer section. For particularly sensitive documents, consider the use of the diagonal watermark. See Section 2 on Protective Markings.

(d) Version Control
There are many ways of expressing the version number on the document, but a standard method is:-
Version 0.1 [Preliminary draft]
Version 0.2 etc. [later drafts]
Version 1.0 [Approved document]
Version 1.1, 2, 3 etc. [Draft amendments]
Version 2 [Next approved version]
Avoid using the phrase 'Final version' – in case it is not!
For the purposes of the folder list, place 'v 0.1' etc. following the name of the document.

(e) Retention and Disposal Schedules
Check the relationship between your work and the official record series that are listed in the Retention Schedule. This will affect how long you need to retain the document.

(f) Folders
There are many ways to organise your folder system, but probably the best is one which explains the relationship of the various functions or subject matter.
Please try to avoid:-

- Using code words, phrases and employee names (e.g. Fred's files)
- Using the name of the Team if you can avoid it. The pace of change in the organisation is such that structures change frequently, while functions continue

Retain the wording of the scheduled Record Series where possible.

Where you have folders which are shared, it is the responsibility of the folder 'owner' to set up any changes.

Your main subject areas should be in one section, and your admin and HR documents grouped in another. The same holds good for grouping your email folders, and it would be a good idea to gradually alter them so that they follow the same lines and have the same names where applicable.

(g) Metadata
This is literally information about information, and provides basic data about your document. In the Microsoft folder structure you can see a pop-up view of some metadata for each of your documents, by hovering your mouse over the file name.

For important items such as policies, you may need to build a metadata section into a front or cover sheet. This would include the name of the person writing the policy, the version number, title, and date of the version. The approval of the draft would also be included. See appendix E for the Document Control Template.

It would be good practice, with regard to documents which are officially scheduled, to amend the Properties entry. For versions of Word or Excel prior to Office 2010, use this routine:-
1. Open the document
2. Click 'File'
3. The 'Properties' is shown on the right
4. You will notice that Microsoft captures automatically the first three words at the top of the page for the Title line. Alter this to reflect the actual title of the document, but you may need to enter a shortened version.
5. Your name should be in the 'Author' line. If the original template or draft has come from elsewhere, someone else's name may appear in this line.
6. Similarly the 'Company' line should state Daventry District Council
7. You may complete the Subject reference if the Title does not cover it precisely. Similarly you may enter some Keywords.
8. Leave 'Manager', 'Category', 'Comments' and 'Hyperlink base' empty, unless there is a specific reason

9. Press Home: this takes you back to the document.

3. Retention and disposal

Retention periods identified within the Retention and Disposal Schedule relate to the information described not the media in which the information is stored. Electronic information should not be stored for longer than necessary simply because it is perceived that it is taking up less storage space. Although electronic storage is relatively cost effective, it is not without cost.

Electronic systems which become too large are proportionately more likely to become corrupted and the speed of the system slows to such a degree that retrieval can become a problem. Therefore, electronic systems should be cleared of unnecessary information on a systematic basis.

Why do we need to do this?

- The short answer is – because we have to!
- The file servers which store all our data fill up quickly, and we need to do some 'housekeeping'
- There is a lot of 'clutter' in our drives and folders, which needs to be pruned out on a regular basis, although not indiscriminately
- Future changes to the IT network (such as Cloud Computing) will require us all to have a leaner, more effective information base

This means that we have to be more efficient in how we use our computers. This applies equally to email, of course: the storage issues are the same. What counts is not numbers of files, but the size of files: how many megabytes they take up. Any file measured in megabytes (Mb) rather than kilobytes (kb) needs regular review.
Examples are digital photographs, scanned images and PDFs (records in portable document format). Deleting a handful of these is as effective as clearing out a whole folder full of Word documents, emails, or spreadsheets.

2. How can we identify what needs to be deleted?

We can do this partly by applying common sense principles, and partly by following guidance which is already available, i.e. within the Retention Schedules. These Schedules exist to govern what we do with our information, and ***apply just as much to electronic information as they do to paper***.

If the records you identify as being out of date are part listed within the Retention Schedule, then you will need to follow the special guidance on disposal or archive.

What about common sense principles? Well, this is about reducing anything which is not part of an official series, and retaining only what is vital for your current work. There are some things you can do fairly quickly and simply to manage the megabytes. Here are some 'quick wins':-

- **Items received from outside DDC**: people often download documents from other organisations, e.g. lengthy policy documents and reports from Government departments.
- **Anything over three years old** may well be out of date, and if you have not used it recently, it is a candidate for review and deletion
- **Employee meeting minutes**: In few cases do we need to keep minutes of ordinary employee meetings for more than three years, refer to the Retention and Disposal Schedule for details.
- **Appraisal forms and notes**: the Schedules say these should be deleted after six years, to comply with Data Protection legislation. If you are a line manager this applies to appraisals you conduct for your employees, as well as those you receive yourself
- **Digital photographs**: transfer any images which are personal property to your home computer as soon as possible and delete them from your work machine. Delete also any work images which are not required for valid or current work purposes. Digital images take up more space than most items on the system, and need careful control: the more you can safely delete the better. Alternatively, explore ways of compressing or converting them to other formats where practical, to save the megabytes.
- **Scanned images**: these are also, in many cases, very wasteful of disc space, sometimes running into megabytes. Are they all needed?
- **Working papers**: Most of us keep electronic drafts and notes of some kind for minor projects and short-term pieces of work. People also often hold duplicates, which are of temporary use only. None of these needs to be kept for more than five years, and many could be deleted long before that. Consult your line manager if you are unsure about the relevance of specific files

These are some of the categories which will give the best results. You should also try reducing numbers of old PowerPoint presentations, and also the contents of your personal drive.

Do we have to log our disposal actions?
Yes, any record identified in the Retention and Disposal Schedule that is disposed of must be logged, to complete the audit trail. There is a disposal register template located at appendix D. This documentation is needed, so that if you are asked to say when a file was destroyed you can give the details, e.g. if there should be a request under Freedom of Information.

Are there circumstances in which we have to retain these items?
Yes. Any records relating to matters which you know to be the subject of an official request for information (Freedom of Information, Data Protection, Environmental Information Regulations) or part of an Audit investigation has to be kept available for use in satisfying the request. Once the request has been received, all disposal activity on relevant records must be halted, or there may be serious legal or disciplinary consequences.

Does this guidance also relate to e-mail?

Yes, both for messages and attachments. The Retention Schedules apply to all formats. If you have a long run of official emails to delete, forming part of a record listed within the Retention and Disposal Schedule, you can summarise the contents in the disposal register.

If someone leaves the authority, what should happen to their records?
As soon as a decision is made, the leaver should discuss this matter with the relevant line manager, involving email and paper records in the arrangements that are made. Any records not in a shared area should be assessed. Those items which are part of a Retention Schedule, or which relate to ongoing business should be transferred to someone else's system, and any personal material must be taken off the account before the date of leaving. Other items should be deleted. The line manager should check at intervals during the notice period that these actions are being done.

What about IT backups?
The Council backs up its data regularly. Back up data is a copy of official information held electronically by the Council. This information is merely a copy of the original data and should be disposed of after one year. Back up information should not be held indefinitely. The original information should be kept in line with the Retention and Disposal Schedules and the backup disposed of.

4. Controlled access to IT Systems

Who controls access to IT systems?
Across the Council there are many IT systems that are deemed under the control of one or more Service Managers. Whilst IT Services are responsible for providing access to the corporate network and core systems of the authority (following manager approval), thereafter it is the responsibility of Service Managers (in their role as Information Asset Owner) to ensure a user's access to a system is controlled and appropriate to their position and role within the authority. Service Managers generally delegate the role of "systems administrator" to another officer within their team.

A list of the expected controls include the following. Service Managers in their IAO role should ensure that:

- An access control policy has been established.
- System administrators have formally been assigned responsibility for an IT system
- Procedures ensure that system administrators are notified of any employee changes
- Users' access rights and permissions are regularly reviewed
- Access to system audit tools is restricted
- Access rights to update parameter data are adequately controlled
- Sufficient employees are trained in the system administration function

Appendix A

Legislation

Data Protection Act 2018	· Statutory Notification of data collection and processing · Information captured for defined legal basis · Communication of privacy notices · Only capture and retain relevant personal information · Keep records up to date · Keep and/or store records no longer than necessary · Respect data subject's rights to have data corrected or removed from system · All information to be kept securely · Data sharing arrangements need to be explicit
Freedom of Information Act 2000	· Applies to current and retrospective (past) information we hold · Make information sources accessible · Self-service access to information where feasible · Open, visible and accountable decision making · Reports written as if already in public domain and open to scrutiny · Members of the public have the right of access to non-personal information · Some legal exemptions apply, such as national security. For most exemptions, Public Interest Test must be considered · Offer advice and assistance to enquirers · Offer a formal complaints procedure · Arrangements for transferring requests that do not relate to the District Council · Arrangements for consultation with third parties
Human Rights Act 1998	· Respect for rights and freedoms of Authority and Individual · Balance private and public interests – individual organisation, community's interests · Public confidence in local government information · Promoting unity in multi-cultural society · Set of binding values upon all society/work communities · Balancing interests of privacy and freedom of expression · Government/public bodies dealing with individuals · New culture of rights and responsibilities · Right to fair treatment in hearing or dispute resolution; zero bias in preparation of evidence
Local Government Act 1972	· Making specified groups of records available for public research after their business life ends.

Standards and Best Practice

These are the standards that were drawn upon to build the Information Handling Practices guidance.

ISO15489	· Adoption of Corporate wide policy statement signed at Management Board level and setting out all employees' responsibilities for record keeping · Corporate wide procedures and systems · Business-based file classification · Managed Record Capture and Managed Retention · Protection of Recorded Information and Defined Access Authorisations · Reliable and correct storage facilities · Correct and complete disposal of records · Policies and procedures reviewed at specified intervals
ISO 17799	· A Corporate wide IT Security Policy Statement, ratified by Members and setting out framework for ensuring all computer systems and data are secure · Assigned responsibilities – custodians of information are responsible for its safe keeping · Security awareness programme and training · Procedures to notify and prevent security breaches · Comprehensive control against computer viruses · Business continuity planning in all business units · Control of proprietary copying respecting owners copyright · Safeguarding of records necessary for the organisation's immediate and long-term survival · Protection of personal data held by the Authority · On-going monitoring of compliance with this policy

Appendix B
Retention and Disposal Schedules

Available via Davnet.

Appendix C

Record keeping systems

Each team must have in place a record keeping system (paper or electronic) that holds its records securely and provides for quick and easy retrieval of information. It must also take into account the legal and regulatory environment specific to the team's function, which is outlined in the Retention and Disposal Schedule.

The system will include:

- Records arranged and indexed in such a way that they can be retrieved quickly and efficiently. This will mean most correspondence-type records having a primary classification of the business activity and date, with other 'metadata' entered as required.
- The ability to cross reference electronic and paper records.
- Titling, indexing, version control and security/protective markings – see appendix E for a document control template.
- Procedures for keeping the system updated.
- Documentation of this system and guidelines on how to use it.
- Procedures covering the treatment of any special media records (eg photographic film) used by the team.

In relation to paper files, the system must be maintained so that the records are properly stored and protected, and can easily be located and retrieved.
This will include:

- Ensuring that adequate storage accommodation is provided for the records.
- Using office space and/or off-site storage effectively (keeping a fair balance)
- Monitoring the movement and location of records so that they can be easily retrieved and provide an audit trail.
- Controlling access to the information.
- Identifying vital records and applying appropriate protection, including a business recovery plan.
- Ensuring inactive records are transferred in a controlled manner to their designated file store.

Appendix D

Disposal register

Retention and Disposal Schedule reference	Records series description	Dates covered	Date reviewed	Reviewed by (Name)	Destruction certificate reference
e.g. IC(1)(2)	*Data Protection Policies and Procedures*	*Superseded policies from 2003*	*Aug-11*	*V Smith*	

Appendix E

Document control template

Organisation	*Daventry District Council*
Title	*Information Handling Practices*
Author	*Vikki Smith*
Filename	*Corporate Records Management*
Subject	*Records Management*
Protective Marking	*NORMAL or CONFIDENTIAL*
Review date	*Dec-12*

Revision History

Version	**Revision Date**
1	*04/05/2010*

Document Approvals

This document requires the following approvals:

Sponsor Approval	**Date**
Senior Management Team	

Document Distribution

Distributed to	**Date**
Council wide	