Information Security Document

Information Asset Management Policy

Version History			
Version	**Date**	**Detail**	**Author**
1.0		Completed for distribution	
1.0		Approved by Information Governance Group	
2.0		Reviewed by Information Governance Group	
3.0		Reviewed by Information Governance Group	
4.0		Reviewed by Information Governance Group	
5.0		Reviewed by Information Governance Group. ICT changed to Information, Notebooks added, classification of removable media.	
6.0		Reviewed by Information Governance Group.	
7.0		Reviewed by Information Governance Group. ISO standard updated. IGG responsibility updated. Information classification added.	

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.6.2.1	Mobile device policy
A.8.1.1 >3	Asset management
A.8.2.1 >2	Information classification
A.8.2.3	Handling of Assets
A.8.3.1	Management of removable media
A.8.3.2	Disposal of media
A.11.2.1-7	Equipment security
A.12.5.1	Installation of software on operational systems
A.17.1.3	Verify, review and evaluate information security continuity
A.18.1.3	Protection of records
A.18.2.2	Compliance with security policies and standards

1 Introduction

Derbyshire County Council recognises the importance of ensuring its information assets are identified and adequately protected. The Council must ensure all information assets are accounted for and maintained appropriately in accordance with its Information Security Management System (ISMS) and by the implementation of good working practices, policies and procedures.

2 Purpose

The purpose of this policy is to ensure that all Derbyshire County Council's information assets are identified, recorded and managed in accordance with the ISO27001:2013 standard and ISO27002 code of practice for information security controls.

The Council categorises information assets as:

- **Information and Information Systems:**
  - Databases
  - Data files
  - Hardcopy documents
  - User guides
  - Notebooks
  - Training material
  - Policies, Procedures
  - Business Continuity plans
  - Financial Data
- **Software:**
  - Applications
  - System software
  - Development software
  - Utilities software
- **Physical:**
  - Computer equipment
  - Communications equipment
  - Portable and local Media – storage and recording
  - Property and accommodation
- **Services:**
  - Communications
  - Utilities (power. lighting, environmental controls)
- **Personnel:**
  - Knowledge
  - Skills
  - Experience
- **Intangibles:**
  - Reputation

3 Scope

This scope of this policy extends to all Council departments, employees, elected members, third parties, vendors and partner agencies who utilise or who are responsible for the development, management and maintenance of all Council information assets.

4 Policy Statement

The Council's Information Governance Group (IGG) co-ordinates responsibility for the management of information assets by appointing nominated information asset owners across departments. All identified information assets must be recorded and managed by information asset owners in accordance with the Council's Information Security Management System.

The Council must take the following steps to ensure all information assets are appropriately identified, recorded and maintained:

4.1 Information and Information Systems

Information held and maintained by the Council can either be in hardcopy form stored in physical locations, filing systems, office locations or stored electronically using software and electronic backup systems.
The Council's Information Safe Haven document (link provided below) gives clear guidance and information on all aspects of storing information and data regardless of the form it takes.

Types of Information and Information Systems assets:

- **Databases** – Access to these must be given to authorised employees only and logs should be maintained to record all access to and changes made to any data held within any database system.
- **Data files** – Access to any data file(s) must be given to authorised employees only and logs must be maintained to record all access to and changes made to any data held within database systems.
- **Hardcopy documents** – All hardcopy documents containing sensitive and personal information must be accessed, processed, maintained and securely stored in accordance with the Council's Information Safe Haven guidance. Restricted hardcopy documents requiring controlled access must have a signing in/out record maintained wherever appropriate.
- **User guides** – All user guides which assist and aid in the understanding of processes, procedures or systems should be safely stored and should be easily and readily accessible to all relevant employees – wherever possible. Guides which exist only in physical form should be digitised to include an electronic version which can be stored electronically on the Council's ICT Network and disseminated wherever possible on the Council's intranet (Dnet).
- **Notebooks** – Information contained in notebooks which are used to record sensitive or personal information must be transferred to secure information systems as soon as possible and either the pages or entire notebook must be securely destroyed once the information has been transferred.
- **Training material** – All relevant training material(s) must be stored and made readily accessible to all relevant employees. Duplication or physical reproduction of training manuals must be kept to a minimum and avoided wherever possible.
- **Policies and Procedures** – All Council Policies and Procedures should be made available and disseminated via the Council's Intranet (Dnet) – All original copies of Policies and Procedures documents whether electronic or hardcopy must be safely stored, regularly reviewed and a version history

control record must be maintained for each document to ensure they are up to date.

- **Business Continuity plans** – All Business Continuity plans must be regularly reviewed, disseminated to appropriate employees and stored safely for easy retrieval as and when necessary.
- **Financial Data** – Data and Information relating to Council financial data must be restricted to authorised employees only. Recording mechanisms must be in place for logging access, changes and use of financial data and information.

4.2 Software

Computer and IT systems software is widely used across the Council and is vital to the day to day running of the Council and in providing essential services to the public.

The use of software has continued to change the way the Council works. Substantial investment has been made in Software along with accompanying ongoing costs and expenditure such as annual software/systems support, licensing and staff training.

- **Applications** – Software used by the Council must be appropriately sourced using Council approved suppliers and must be evaluated for business need, suitability, efficiency, ease of use, cost effectiveness and integration into existing Council systems. All software approved for use by the Council must be recorded on an approved software list. Appropriate numbers of software licenses must be purchased to cover volume of use and to satisfy legal requirements. Software media must be stored (physically and electronically) in a secure, centralised location along with software installation codes and registration numbers. Access to software media by employees must be controlled and limited to authorised employees only. A record must be maintained of all installations of software, licensing volumes SLA documentation and references in a centralised location where access is provided to authorised employees only. A signing in/out system should be used for controlling the use of physical software media.
- **System software** – Server/system software such as Operating Systems, must be evaluated for business need, suitability, efficiency, cost effectiveness and integration into existing Council systems. Operating System installation media must be stored in a secure, centralised location along with installation codes. Access to Server/system software media by employees must be controlled and limited to authorised employees only. A record must be maintained of all installations of software, licensing volumes SLA documentation and references in a centralised location where access is provided to authorised employees only. A signing in/out system should be used for controlling the use of physical software media. Backups of complete Server/systems installations must be routinely carried out for disaster recovery purposes. Installation, configuration and maintenance of Server/system software must only be undertaken by employees who are trained and qualified to do so.
- **Development software** - software for the support of existing systems and for the development of in-house solutions must follow the same processes for procurement and use as for the applications and Server/systems software. Development software should only be used by employees who are trained or who are undergoing training to use the development software.

All types of software (with the exception of routine security updates and patches verified by software vendors) must go through agreed purchasing procedures and must be recorded on a Council approved software list.

4.3 Physical

The Council's most visible information assets are those which are physically located throughout the Council such as computers, printers and phones etc. Offices and buildings must also be considered as information assets – providing location for the housing and installation of the Council's ICT Data and Communications Network infrastructure and physically stored documents and information.

- **Computer equipment** – A large number of computing devices are in use across the Council. Computers are one of the most costly single items of equipment and must be subject to controls from procurement to disposal. The Council must be able to track all activity and use relating to all Council computing devices using various means such as via the computer network and/or using logging systems such as signing in and out and other such recording mechanisms. All computers must be allocated a unique asset tag number which is recorded against the manufacturer's serial number and model which should never be altered or exchanged with any other computer. Each computer must have the tag number securely located and easily visible on its outer casing along with the standard Council security etchings. Throughout its life, a computer may be subject to hardware upgrades, new software installations, configuration changes and maintenance and all such activity must be appropriately recorded, maintained and updated by the Transformation Service.
- **Communications equipment** – Mobile and office phones are widely used communications devices across the Council. Other network and communications devices identified as information assets include routers, switches, video conferencing equipment etc. Along with computing equipment, these devices must be allocated an asset tag number which is securely located and easily visible on the device. All communications equipment must be identified, recorded and appropriately maintained by the Transformation Service.
- **Portable, local media storage** – Media such as CD/DVDs, Magnetic tape, flash/portable hard disks are valuable information assets because they are used to save and retrieve Council information and data. Irrespective of the information stored on them, all such media must be classified and handled as 'RESTRICTED' in accordance with the Council's Information Classification and Handling Policy. The portable nature of this type of media requires responsible use and adherence to all Council policies, procedures and processes which are in place for the protection of information and data. Appropriate labelling and recording mechanisms should be in place to ensure the safety and integrity of media - enabling tracking of essential media such as for data backups e.g. media required to carry out data/file restores must be signed in and out from a secure location. Portable media must be used in accordance with the Council's Encryption Policy, Desktop and Mobile Device Procedures and Data Protection and Media Handling Procedures:

All physical computer, communications and storage media/devices must go through agreed purchasing procedures and must be recorded on a Council approved hardware inventory.

- **Property and accommodation** – The Council's Corporate Asset Management Plan provides comprehensive information relating to buildings and property as information assets. ICT equipment along with Data and Network Communications infrastructure equipment is housed in many buildings and property owned by the Council and is therefore subject to the Corporate Asset Management Plan:

4.4 Services

- **Communications** – It is vital for the Council to maintain its ability to communicate in many different forms. Communications equipment must be maintained and clear processes, policies and procedures for the provision of this service must be in place. E-mail is also a vital means of communication and as such, requires a robust, reliable infrastructure to enable the Council to communicate effectively and reliably, both internally and externally.
- **Utilities (power. lighting, environmental controls)** – These services are information assets as they provide fundamental requirements for the Council to function appropriately, safely and effectively. It is essential that property maintenance and inspections are routinely carried out and that employees are proactive in reporting faults, whenever noted, to the Council's Property Services division.

4.5 Personnel

The Council cannot function without its workforce – it is its largest asset. The provision of good public services requires Council employees to have the necessary skills, knowledge and ability to work within many different areas and departments across the Council. The number of unique functions and specialisms across the Council requires a varied knowledge and skills base which must be supported by robust recruitment processes, appropriate training provision and good management of employee skill identification, work placement and allocation.

- **Knowledge and Experience** – The Council has a great pool of employees who have a wide knowledge and experience base to draw on and as such, is a valuable information asset.
- **Skills** – All Council employees must possess the necessary skills and ability to do their jobs.

4.6 Intangibles

- **Reputation –** The Council is very aware that public perception and confidence in its ability to deliver effective, efficient public services is of the utmost importance. Reputation is an asset which promotes confidence and generates support in what the Council is trying to achieve. The Council takes its reputation seriously and proactively engages to develop policies and procedures along with a consistent approach in maintaining and presenting the right image.

  The Council encourages good reputation and is assisted by:

- Good working practices: http://dnet/policies_and_procedures/human_resources/code_of_conduct_for_employees/default.asp

- Corporate Image Branding: http://dnet/resources/council_branding/default.asp

- Putting People First charter: http://dnet/working_for_us/customer_care/putting_people_first/default.asp

- Public Consultation: http://dnet/what_were_doing/consultation/corporate_consultation_group/default.asp

4.7 Information Classification and Handling

All Council information has a value to the organisation, however not all of the information has an equal value or requires the same level of protection. Being able to identify the value of information assets is key to understanding the level of security that they require.

The Council maintains an Information Classification and handling scheme which involves grouping information and categorising content to establish the most appropriate way of handling, storing, retrieving and to determine who is authorised to access particular Information.

All information in both electronic and physical forms must be categorised using either '**PUBLIC**', '**CONTROLLED**' or '**RESTRICTED**' and must be appropriately labelled. Any information that is not specifically marked as being 'RESTRICTED' or 'CONTROLLED' will be deemed to be 'PUBLIC'.

Where information is grouped together, the **highest** classification must be applied to all information in the group.

The Council's information classification and handling policy and procedures provide further information and can be found here:

http://www.derbyshire.gov.uk/working_for_us/data/document_classification/default.asp

5 Acceptable Use Of Assets

All Council departments, employees, elected members, contractors, vendors and partner agencies must observe and abide by all Acceptable Use policies and procedures pertaining to all Council owned information assets.

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council’s security procedures and policies.
All Council employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council’s Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

This document forms part of the Council's ISMS Policy and as such, must be fully complied with.