CABINET

THURSDAY, 11 SEPTEMBER 2014

REPORT OF THE PORTFOLIO HOLDER FOR OPERATIONS AND ASSETS

CORPORATE RECORDS MANAGEMENT POLICY

EXEMPT INFORMATION

None

PURPOSE

To seek approval from Cabinet for the Corporate Records Management Policy

RECOMMENDATIONS

That Cabinet approves the Corporate Records Management Policy and adopts it as a Council Policy

OPTIONS CONSIDERED

Options that have been considered are ;

1. Do Nothing
2. Adopt the Corporate Records Management Policy

Option 2. Adopt the Corporate Records Management Policy is the preferred option.

RESOURCE IMPLICATIONS

There are no direct financial resource implications to the adoption of this Policy

LEGAL/RISK IMPLICATIONS BACKGROUND

The risks of not adopting this Policy are significant, given the Council's obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000. Responses from the Information Commissioner for breaches of either of these Acts could run into significant figures.

The added reputational harm that would undoubtedly arise from such a circumstance would be very difficult to repair, causing the Council embarrassment and losing the confidence of those citizens and customers about whom we hold information and data.

SUSTAINABILITY IMPLICATIONS

There are no Sustainability Implications.

BACKGROUND INFORMATION

Records are defined as recorded information (irrespective of medium or format) which are created, received or maintained by the Council in pursuance of our legal obligations or in the transaction of our business.

There are various governance, code of practise and government circulars that dictate best practise in the field of Records Management, however, all local authorities have obligations to fulfil provisions under both the Data Protection Act 1998, and the Freedom of Information Act 2000, to ensure data is ;

- Used in a way that is adequate, relevant and not excessive
- Kept for no longer than is absolutely necessary

Whilst there are mechanisms in place in many of our corporately used systems, an element of this management needs to be performed manually. Additionally, where mechanisms do not exist, the full process is performed manually.

The Acts specifically dictate that Local Authorities need to provide a clear basis to determine what information is retained by the organisation and is therefore consequently accessible under the Acts.

The Council is additionally progressing the electronic storage of documentation through the Electronic Document and Records Management System (EDRMS) and it is necessary to determine the parameters for the management of such information, including the retention period for such data for inclusion in the ongoing configuration of this system.

It is recognised that a Policy such as this is a key component of good corporate governance. It demonstrates the Council's commitment to undertaking its business activities in a diligent and accountable manner and helps communicate this commitment clearly and effectively to stakeholders.

REPORT AUTHOR

Nicki Burton, Director – Technology & Corporate Programmes

LIST OF BACKGROUND PAPERS

None

APPENDICES

Appendix A – Corporate Records Management Policy

APPENDIX A

IS 92246
ISO/EIC 27001:2005

Records Management

RECORDS MANAGEMENT POLICY

Document Hierarchy: Tier 1 Policy

Document Status: Final

Document Ref: DOC 15.2

Originator: D Bolton

Updated: D Bolton

Owner: Corporate Information Security Manager

Version: 01.02.01

Date: 30/01/12

Approved by Corporate Management Team

Classification: Unclassified

Document Location

This document is held by the Council, and the document owner is Derek Bolton, Corporate Information Security Manager.

Printed documents may be obsolete, an electronic copy will be available on the Council's Intranet. Please check for current version before using.

Approvals

Name or Group Lead	Title or Approving Group	Approved
Tony Goodwin	CMT	Yes
Derek Bolton	Security Management Group	Yes
Nicki Burton	ICT Management Team	Yes

Approvals

This document shall be presented to each group for consultation and approval.
ICT Management Team for technical approval
Security Management Group for departmental approval
Corporate Management Team for organisational approval

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and access by authorised users.

Security Classification

This document is classified as UNCLASSIFIED with unrestricted access to Council Staff and business partners.

CONTENTS PAGE

1 INTRODUCTION

1.1 Records are recorded information (irrespective of medium or format) which are created, received or maintained by the Council in pursuance of our legal obligations or in the transaction of our business.

1.2 Records management is central to our business. It is a programme to control records throughout their life, from creation to final disposal. It will ensure that unnecessary records are not created, that necessary records are used and stored effectively and economically, and that records which are ephemeral or whose use has ceased after a certain time are destroyed at the earliest possible opportunity. In addition, it will ensure that records of lasting value to the Council and wider community are preserved permanently.

1.3 There are various Act, Statutory Instruments, Government Circulars, International / European / British standards and codes of practice as well as professional advice from the Records Management Society that affect the work of Local Government and record keeping. This policy document has been produced in accordance with professional principles and practices with this statutory guidance in mind.

2 RESPONSIBILITIES

2.1 The Chief Executive has overall responsibility for records management issues and delegates this function to the service area directors.

2.2 The Corporate Information Security Manager within ICT has overall responsibility for delivering records management for the Council.

2.3 The Director – Technology & Corporate Programmes, in conjunction with the Portfolio Holder – Operations and Assets, deliver the strategic direction for Records Management

2.4 The Service Area Managers have the day to day responsibility of managing records with their own service areas.

3 OBJECTIVES

3.1 The Council's records management policy will be required to achieve the following objectives:

- To ensure effective and economic management of Council records;
- To provide security for confidential information;
- To enable use of the records as an information source;
- To ensure business continuity;
- To ensure compliance with the law;

- To ensure legal admissibility and evidential weight;
- To ensure the transfer of records with historical significance to archives.
- To support an agile and flexible workforce

4 SCOPE

4.1 RETENTION SCHEDULE

4.1.1 Each service area must have a retention schedule governing their records. The Records Management Service (RMS) provide guidance on generic retentions based on legislative and audit requirements.

4.1.2 All departments are required to carry out a survey to produce an accurate retention schedule to enable checks to be made on duplication, compliance with retention legislation, storage capacity and ensure that due consideration is given to the long term value of any record series. The absence of a comprehensive list of all related documentation exposes the Council to the risk of prosecution. It is particularly important to identify related records across more than one service area and identical information in more than one format.

4.1.3 The surveys shall be reviewed on an annual basis by service areas and shall be reflected in the retention schedules where modifications are made to take into account any redistribution of functions and changes in record keeping practices.

4.2 FILING SYSTEMS

4.2.1 A filing system is a collection of structured information, retained in any format and used to carry out the business of the Council. All information used to conduct the Council's business, and supplied to other organisations and individuals must be recorded in a filing system.

4.2.2 Although the responsibility for the naming of manual files and file series lies with the relevant service area, a corporate system is used to identify records, and a similar system needs to be adopted for electronic records. This has the advantage of a consistent approach in records management and is contained in a Code of Practice. This consistency assists in the operation of a centralised filing system or repository, where files are managed off site by a third party.

4.2.3 Standardisation of series titles e.g. creditors, invoices, planning applications, repairs, etc. will be in place ensure structure integrity. A structured interlinked directory aids cross referencing of files or data sets.

4.2.4 All new files should be created with the need to avoid duplication in mind.

4.2.5 Confidential records such as personnel and payroll files will continue to be held by individual personnel and payroll teams, whilst there may be special arrangements with regard to the location and accessibility of confidential information.

4.2.6 All file covers should be consistent in their reference and content description and should show as a minimum to whom the information belongs, the subject, retention information and file activity to aid retrieval as described in 4.2.3.

4.2.7 Electronic and digital media must be labelled and located in an appropriate folder.

4.2.8 For retention, destruction and archiving purposes, all record formats are treated under the same rules.

4.2.9 Every service area must include in their disaster recovery plan, protection of records to reduce the impact of an event to ensure information can be recovered. Consideration is required for electronic/digital records and action should be based on a thorough business risk assessment.

4.3 STORAGE

4.3.1 Responsibility for storage rests with each service area, this may be centralised by floor/location or use of approved off site storage. It is not acceptable to use unapproved or ad hoc off site storage such as garages, vacated buildings used also for general storage, etc.

4.3.2 For off site storage to be approved the site must comply with a risk assessment based on security, physical conditions and equipment that will allow effective and safe retrieval of information. The risk assessment will be conducted by the manager of the records to be stored under the guidance of the Corporate Information Security Manager or their representative.

4.3.3 All records in offices must be stored in a safe manner and must not be stored in such a way to cause accidents or injury through lifting. The Safety Officer must be consulted when considering either reviewing existing storage through office moves or when looking at new facilities.

4.3.4 Management review dates should be used appropriately and not as an excuse to procrastinate or to avoid responsibility for action. Review dates should not be continually amended to one in the future without undertaking a proper review.

4.3.5 All records produced electronically should be subject to a back up on a regular basis. The back up medium should be appropriate to the length of time required to store the information. Some inferior types of media tend to degrade quicker than others dependent on the handling, storage and nature of that media.

4.3.6 Document imaging or Electronic Document Records Management System (EDRMS) should be considered if there is a need to:

- Automate workflows
- Integrate document and data processing
- Manage large volumes of active documents
- Provide multi access document handling
- Provide on line document access
- Provide printed copy locally
- Control access to document retrieval

4.3.7 EDRMS shall be governed by the proposals in the *Retention Schedule* the same way as paper records and subject to the same handling and safeguards.

4.3.8 Liaison with Staffordshire County Council may be required where documents are deemed to be preserved where they are considered to be of historical significance to determine the method of how the originals are handled and stored into permanent storage.

4.3.9 E-mail and information stored on a PC or on the network and used to facilitate the performance of Council work is a corporate asset and a critical component of the Council's communications, therefore this will be treated in the same manner as any other information format.

4.4 CATEGORIES OF ACCESS

4.4.1 All information must have an access category that will determine the level of protection from unauthorised viewing and usage in accordance with our *Information Security Classification Policy*.

4.5 DISPOSAL OF RECORDS

4.5.1 Records must be retained and disposed of according to the Council's *Retention Schedule* and the *Retention of Records Policy*.

4.5.2 Information no longer required must be destroyed in accordance our legislative responsibilities and appropriate to the access level in 4.4.1 afforded to that information.

4.5.3 Media containing information must be destroyed in accordance with our *Disposals of Equipment and Media Policy.* Further guidance can be sought from ICT Services.

4.6 RECORDS OF ARCHIVAL VALUE

4.6.1 There are a number of records that have archival value, irrespective of the medium on which they are stored. These could include records that contain historical/genealogical/local history and social science information that may be of use to future historians or researchers for the study of social, economic and political issues. There are also records that the borough needs to keep in order to provide evidence and justification for its actions in the past.

4.6.2 Managers may need to seek guidance and advice off the County's Archivist to ascertain the most appropriate method of handling and storage of such information to ensure its permanency and future accessibility.

4.7 RECORDS MANAGEMENT DEPARTMENTAL RESPONSIBILITIES

4.7.1 Each service area must nominate an officer who has the responsibility for ensuring their obligations are met in respect to managing records in accordance with this policy and its related documents.

4.7.2 This register shall be maintained by the Corporate Information Security Manager.

End of Document