HARINGEY COUNCIL

RECORDS MANAGEMENT POLICY FOR ELECTRONIC RECORDS

## 1.	PURPOSE AND SCOPE OF THE POLICY

This policy complements Haringey Council's Records Management Policy. It aims to meet the requirements of good records management to cover the electronic records of Haringey Council. The policy covers:

- The requirements that must be met for the records themselves to be considered as a proper record of the activity of the organisation;
- The requirements for systems and processes that deal with records, the quality and reliability of which must be maintained to provide a valuable information and knowledge resource for the whole organisation;
- Its place within the strategic and policy framework of the organisation;
- The implementation plan across the organisation;
- The use of approved technical solutions;
- The resources needed to preserve the record intact;
- The policy governing Registration process;
- The policy governing access;
- The policy governing security;
- The policy for reviewing the policy and checking the quality of implementation.

These will be updated according to a development plan issued within the policy making areas of Haringey Council.

## 2.	MEANING OF RECORDS AND NEEDS FOR RECORDS IN HARINGEY COUNCIL

For the purposes of this document, an **electronic record** is defined as:

Recorded information, created, received or held in electronic format, which provides reliable evidence of Haringey Council policy, actions or decisions.

The policy covers all records created and received by all departments of the Council in all electronic formats, including documents:

- Stored on computers;
- Stored on mobile storage devices, such as tapes, discs, CD's, memory sticks, mobile phones, PDA's;
- Transmitted across networks;
- Sent by fax;
- Sent or received by e-mail;
- Sent or received by (SMS) text message.

This policy is complemented by a suite of policies, based on ISO 27001 2005 *Code of Practice for Information Security Management*, dealing with various aspects of the management of electronic records. These are:

- AUP001 Email Acceptable Usage Policy
- AUP005 Data Protection Policy
- AUP006 Portable Storage Device Acceptable Usage Policy
- AUP007 Data Storage Acceptable Usage Policy

- AUP008 IT Data Retention Acceptable Usage Policy
- IPR007   Information Handling, Labelling and Disposal Procedure
- ISP003   Information Classification Policy
- ISP010   Compliance Policy

3. REQUIREMENTS FOR RECORDS MANAGEMENT

Electronic records within Haringey Council are to be clearly identified following a pattern of treatment similar to that previously given to paper records. They must be able to be preserved, and stored for the required period within Haringey Council. They will be selected using defined selection criteria and can be transferred to other organisations for future preservation, or destroyed once they are no longer of operational use.   In order to ensure that the information constitutes a record, Haringey Council is required and endeavours at all times to ensure that:

- The record is present
  The information needed to reconstruct activities and transactions that have taken place is recorded
- The record can be accessed
  It is possible to locate and access the information and present it in a way that is true to the original presentation of the information
- The record can be interpreted
  A context for the record can be established, showing when, where and who created it, how it was used and how it is related to other information
- The record can be trusted
  The information and its representation exactly matches that which was actually created and used, and its integrity and authenticity can be demonstrated beyond reasonable doubt
- The record can be maintained
  The record can be deemed to be present and can be accessed, interpreted and trusted for as long as necessary and on transfer to other approved locations, systems and technologies

4. PRINCIPLES

Haringey Council deems that electronic records are an asset that requires careful control and the diligent application of standards to all systems and processes within the organisation. The systems and processes will be required to:

- Identify whether they deal with records, electronic records or potential electronic records;
- If they do deal with such records, the system or process must maintain them so that the record nature remains intact;
- Provide information on the records or potential records as required for inclusion as part of a collection in the inventory of record collections;
- Provide the records for registration, transfer or disposal according to the records management guidance;
- Keep the records secure and monitor access in accordance with records management guidance;

- Have regard for legal requirements such as Data Protection, Freedom of Information and copyright legislation.

Haringey Council will monitor electronic records and potential electronic records to ensure that:

- Records that should be captured are being processed electronically if they do not appear in the paper record;
- There is no unwarranted duplication between the paper and electronic record collections;
- There is a distinction made between the electronic documents which are printed, printed records that reside in the paper record systems and other original documents that are retained as electronic records (possibly to be passed to an electronic record keeping system);
- An inventory of record collections will be created to ascertain the nature and type of records and potential records within collections. Care must be taken to ensure a good level of control of the record creating systems and that the record's nature is preserved appropriately in the transitional period.
- The implementation of any Record Management System should clearly show where the record is located and in which form it is held.

5.   POLICY FRAMEWORK

There will be requirements in other policies that electronic records must meet. The following are made specific by reference:

- Following best practice
  Electronic records will be managed in accordance ISO/CD 18489-1, which provides an overall guide to best practice in records management
- Haringey Council's e-business strategy
  Electronic records will underpin e-business providing records for business use, corporate knowledge management and evidence-based policy making, evidence for accountability and historical use
- Freedom of Information Act
  Electronic records will adhere to procedures under the Freedom of Information Act and the associated Lord Chancellor's Code of Practice on the Management of Records
- Data Protection Act
  Electronic records will have to adhere to procedures under the Data Protection Act 1998
- Existing records management policy and associated policies, including those set out in Section 2 above
- Audit policy
  Electronic records will meet Haringey's audit requirements

6. TECHNICAL POLICY

Haringey Council applies technical criteria to the technologies that process electronic records. This ensures that:

- It is technically possible for the electronic records to meet record requirements, starting from when they are created and for as long as they are needed; however, there are some legacy applications that may not be able to meet this criteria at present;
- Systems will be selected on the basis of how well they will cope with electronic records, to prevent any loss of the record because of incompatibility or insufficient safeguards being sued;
- Records management systems adhere to the minimum functional requirements as stated in the PRO publication *Functional requirements for electronic Records Management Systems*;
- The systems designed for records management are capable of and useful for record keeping activities;
- Metadata are captured and can be used for referencing the information by using defined terms that are user- friendly and accurate.

7. PRESERVATION POLICY

Haringey Council seeks to preserve electronic records during any change in the infrastructure so that they can still satisfy the original policy requirement. Preservation needs must be satisfied when there are changes in:

- The technology that processes the electronic records how this affects the way records are processed throughout the records' existence;
- The definition of terms used in the metadata and within the records themselves;
- The classification of the electronic records including how the records are grouped and described so that they can be presented in a way consistent with the original understanding of the subject when the record was created.

8. REGISTRATION POLICY

The registration of electronic records will follow best practice in records management and allow for the users of the records to identify and track particular records and record collections.

The approach Haringey Council has to registration involves:

- Classifying the records into series that have meaningful titles and a consistent reference code;
- Setting a responsibility on individuals forming record items to allocate them to a series and if necessary a sub-series or sub-sub-series;
- Having sequences of reference numbers that can cover series with both electronic and paper records;
- Checking that the correct records have been allocated to the sequence and that meaningful titles are used;

- Auditing lists of the references used so that the registration system makes sense and records can be found in appropriate search sequences.

9.   ACCESS POLICY

Haringey Council will use access controls to allow the records to be viewed by all relevant parties, and offer a mechanism for opening up some of the information for use outside this group.

The actual controls will depend on many factors but the general principles can be summarised as:

- Electronic records will be made available for continuity of actions.   The creators and managing individuals or groups should have access to relevant information.
- Haringey Council's Policy & Performance team, which has been identified as being able to make an accurate judgement, will decide on the sensitivity of the record.   This judgement may be on a whole series or simply cover individual items.   It will identify any restrictions on the records and it will highlight any groups or individuals within the organisation who should have access.
- Any judgements, including any background reasons for withholding or masking information within the record or record series, are to be recorded. The resulting record will be kept for at least as long as the records in question; however, it may not have the same access status as the main record.
- Haringey Council will not seek to put blanket restrictions on a record series if only some of the individual records are judged sensitive.
- Electronic records are subject to the Public Records Act 1958 and Haringey Council will ensure that they are treated accordingly.   Access will be needed for appraisal decisions to be implemented.   The nature of the access will be defined for records judged to be of a sensitive nature.
- Information taken from the records or record metadata may be subject to legislation requiring it to be either withheld or made more widely available outside normal business needs (or even outside the organisation itself).   For example there may be a need for compliance with data protection or Freedom of Information legislation.
- All records are part of the corporate memory.   Unless restricted, due to legislation or as a result of a judgement, they will be made readily available within the organisation. This may be subject to volume restrictions because of technical limitations or copyright reasons.
- Any access arrangements will be made for a specified duration and these will be reviewed according to a schedule identified during appraisal.

10.   SECURITY POLICY

Haringey Council takes all reasonable steps to ensure that the electronic records and processes dealing with them are secure.   Once recorded and registered in the system, they will be safe from alteration, misinterpretation or loss.

The steps include:

- Informing all staff and complying with records management best practice;
- Using a corporate policy and organisational procedures, where they exist and helping to determine new policy and procedures where they do not;
- Training staff to use the records management systems for an accurate representation of the records using only relevant metadata, thereby ensuring consistency in record registration and metadata without loss of context and control;
- Auditing the systems to trace any deviation from procedure;
- Offering solutions to rectify mistakes or altering the procedures to accommodate better ways of working;
- Setting up business continuity plans to ensure a constant service is maintained in spite of any technical or strategic hitches that may occur;
- Enforcing access restrictions with user ID's and passwords, setting user lockouts;
- Maintaining disaster recovery plans that include replication electronic records on a physically secure back-up and safeguarding the information from technical failures;
- Implementing strict back-up cycles with updates for new records and metadata, ensuring that any destroyed or transferred records are also promptly physically cleaned from the back-ups;
- Labelling the replicated records as a replica set and making sure these cannot be used as the master set, unless the original has been destroyed accidentally or following a disaster.

This policy is complemented by a suite of policies, based on ISO 27001 2005 *Code of Practice for Information Security Management*, and listed in Section 2 of this document.

11. POLICY REVIEW

Haringey Council will endeavour to follow the policy within all relevant procedures and guidance used for operational activities. Interpretation of the policy will be monitored and there will be a regular planned audit to access how the policy is being put into practice.

The audit will seek to:

- Identify areas of operation that are covered or not covered by the policy and to identify which procedures and/or guidance should adhere to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of electronic records and use a subsidiary development plan if there are major changes to be made;
- Set requirements by implementing new procedures, including obtaining feedback where the procedures do not match the desired activity;
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures such a security and access.