Safe City Living Lab Privacy Impact Assessment Report

August 2015

Absolutely Positively
Wellington City Council
Me Heke Ki Pōneke

TABLE OF CONTENTS

Introduction

In May 2014, the Wellington City Council and NEC entered into a formal agreement with the aim of exploring how technology can support 'Safe' and 'Smart' City. The collaboration aims to leverage local and global expertise.

In particular NEC and the Wellington City Council were interested in exploring how technology can support solutions tailored to local issues and opportunities. However it was acknowledged that locally delivered projects must be developed in collaboration with partners and key stakeholders.

As a result, NEC and WCC facilitated a number of workshops (initial workshops - November 2014) with broad range of stakeholders. The stakeholders included the NZ Police, Fire Service, Inner City Resident and Retailer Associations, Social Services and community groups, government and health agencies, Wellington Region Emergency Management Office (WREMO) and the Ministry of Defence and Emergency Management (MCDEM).

It emerged from these workshops that there was a common interest in developing a mechanism for:

- evidence based future planning
- enabling a more informed situational tactical response to local incidences and concerns (including support for the city's most vulnerable residents)

It was also agreed that Cuba Mall would provide a unique opportunity for a "Living Lab" approach to test the development of future models.

The Living Lab is a collaborative initiative to explore benefits to the city, government and health partners as well to business and community, using technology in a low risk way.

The living lab model provides the opportunity to test and change quickly, an iterative and agile approach to the development of the project as well as an opportunity to develop a model easily transposed to other locations.

Cuba Mall/Precinct was confirmed as an ideal location to develop a "Living Lab" case study that would provide rich and varied data:

- is a clearly defined geographic location with layers of complexity both in design and street environment
- a diverse range of people and retail and residential activity
- a number of projects already underway with the police, residents and retailers of Cuba Mall and would inform this development

The project utilises existing assets and sources of data and information streamlined, integrated and coupled with new sensory and analytical methods and technologies.

The project adds intelligence to existing data sources such as CCTV feeds and other sources in an anonymised fashion.

The integration of these data sources and transforming them into high value information by location delivers both immediate and longer term outcomes:

Immediate

- A co-ordinated and centralised information management
- An improved alerting and response through situational awareness
- Ability to identified trends and patterns
- An improved efficiency and response of agencies' current day-to-day activity and a multi-agency ability to respond to those in need
- Providing a framework for evidence based decision making and future planning

Long term - targeted/real time responses will provide invaluable insights to assist with:

- Urban design and safe city planning
- Developing sustainable strategies to address social issues
- Providing street level trends to retailers to help maximise retail opportunities
- Assisting in understanding foot-traffic flow which will inform the planning of spaces/places and assist retailers by aligning information to such things peak shopping times.

Description of the project and information flows

We will have two cameras in Cuba Mall- one on the corner of Cuba and Ghuznee Streets on the same pole as the existing WCC CCTV camera, and one on opposite Left Bank Mall on a new pole along with the acoustic sensor. These are not part of the WCC CCTV network and will be in place for the duration of the trial only.

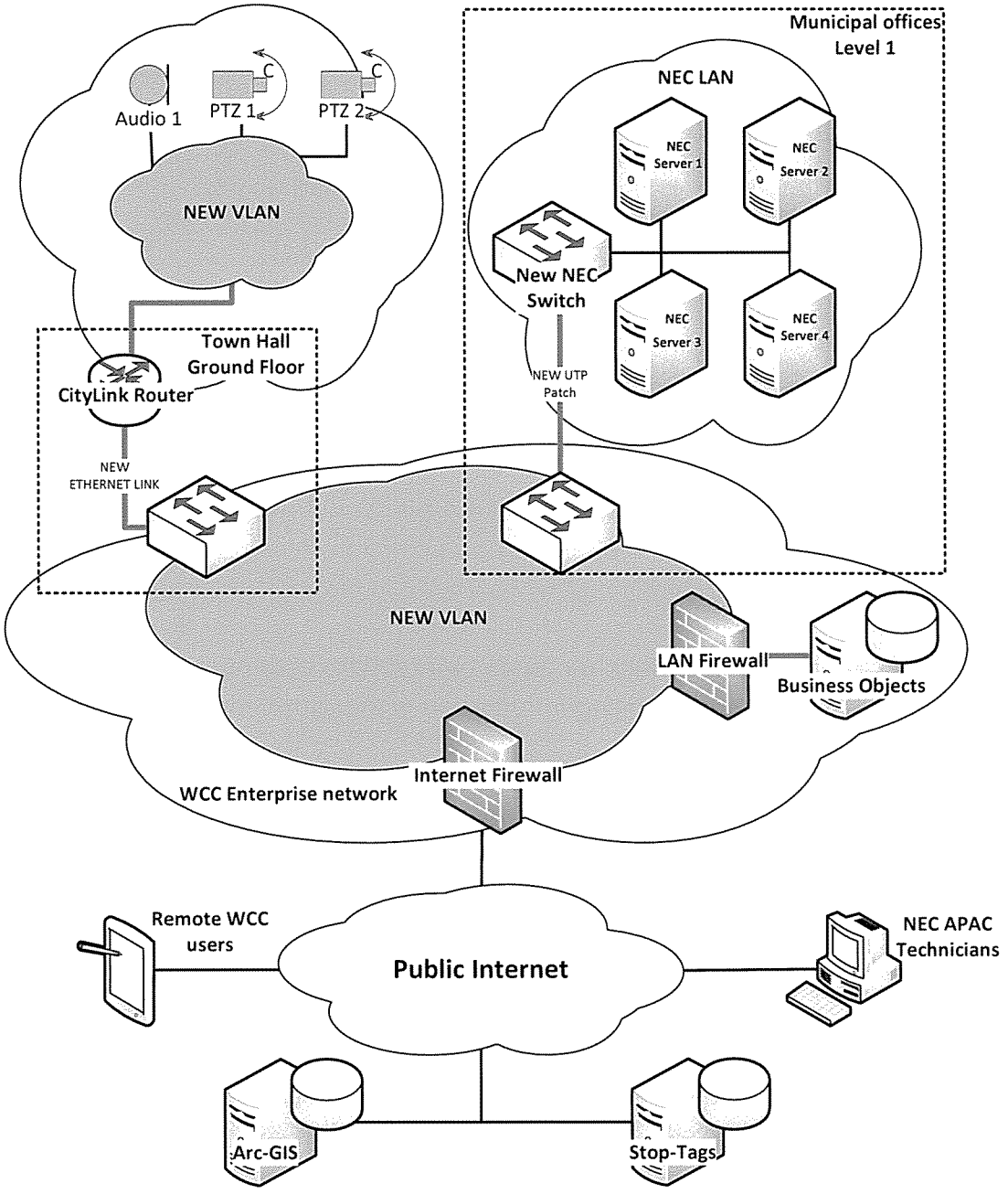
Data from these will be streamed to servers hosted by the WCC Security Office.

This data and other files of current intelligence already collected will be overlaid on a Magic 1c board situated in a secure room in Council and will be able to be viewed by the Community Services and Security Managers.

The events/alerts generated from the surveillance system will provide valuable data to generate actionable insights such as trends, patterns and hotspots.

Briefly, the solution employs video and acoustic analytics for the purpose of human behavioural analysis. Machine learning techniques are employed to detect a number of scenarios e.g. begging, drunken behaviour, unsociable behaviour, crowding and broken glass. When threshold for these behaviours are met then an event is created and populated on the situational display.

The situational display provides the operator with the situational picture around the area of interest. Through the display, the operator can monitor incoming alerts or events, generated by the underlying analytics system. Specifically, the alert provides the operator with the meta-data of the detections. For example, the time and location of detection, type of detections and image/video/audio playback. The display also enables several overlays of information to be presented onto the map. These overlays can also be provided by external 3rd-party data sources through pre-defined message structure and web service interfaces.



The privacy analysis:

The trial will involve the deployment of two fixed CCTV cameras in two locations and an acoustic sensor.

The trial will begin in August 2015 and the outcomes will be evaluated in November 2015.

The trial Living Lab CCTV network is on a secure network separate from the general Council network.

Privacy risk assessment

The Safe City Living Lab trial has been assessed against potential risks.

R1	failing to comply with either the letter or the spirit of the Act	Compliant
R2	stimulating public outcry	Low risk
R3	loss of credibility or public confidence re privacy concerns	Low risk
R4	underestimating privacy requirements	Low risk

While the system does not collect any personal information the public may have a "big brother" perception.

Privacy Enhancing Responses

The camera and acoustic sensor based methods being trialled are not designed to collect personal information. The resulting information is therefore considered to be completely anonymised.

The system will be configured on a separate network and on a separate server configuration to the main WCC or NEC networks. This system infrastructure also supports the WCC CCTV and Traffic management system.

Recordings will be kept for 18 days. Within that time, certain recordings could be archived for evidence purposes if needed.

The recordings are stored on a secure server within WCC premises and can only be accessed via the NEC MAG1C Board terminal that will be securely located within WCC. Access to this terminal will be password restricted and only users with the appropriate access rights will have access to recordings.

The cameras are the property of NEC and will be returned to the company at the conclusion of the trial.

Compliance mechanisms

The trial will comply to the WCC Information Management Standard policy, which covers CCTV Information Request and Public Information Guidelines.

Appendix

The Privacy Act - Information Privacy Principles (IPPs).

The following section examines the trial Safe City Living Lab project impact on and compliance with The Privacy Act - Information Privacy Principles (IPPs).

Principle 1 – Purpose of collection of personal information

Personal information is defined in section 2 of the Privacy Act 1993 as:

"information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former Act."

"Individual", in turn, is defined (again in section 2) as:

"a natural person, other than a deceased natural person."

SOURCE: PERSONAL INFORMATION IN NEW ZEALAND: BETWEEN A ROCK AND A HARD PLACE?
KATRINE EVANS, ASSISTANT COMMISSIONER (LEGAL), OFFICE OF THE PRIVACY COMMISSIONER, NEW ZEALAND

The trial CCTV network is not designed to and does not collect or hold information about an identifiable individual.

Principle 2 – Source of personal information

The trial Living Lab CCTV network is not designed to and does not collect or hold personal information directly or indirectly.

Principle 3 – Collection of information from subject

The subject is the collective inhabitants of and visitors to Wellington.

WCC will reasonably inform the subject by publishing information on the WCC web site.

The purpose of the information is to inform decisions about future planning and situational tactical response to local incidents in Cuba Mall.

The project and outcomes will be summarised and described on the WCC web site.

Principle 4 – Manner of collection of personal information

The information is collected by lawful means.

The information is not collected unfairly.

The means of collection do not intrude unreasonably upon the affairs of any individual.

Principle 5 – Storage and security of personal information

The trial Living Lab CCTV network is not designed to and does not collect or hold personal information.

The trial Living Lab CCTV network is on a secure network separate from the general Council network.

Recordings will be kept for 18 days and stored on a secure server within WCC premises accessible via a terminal located on level 6 of the WCC offices. Access to this terminal will be password restricted and only users with the appropriate access rights will have access to recordings.

These measures provide reasonable safeguards against Loss, Access or Misuse of the information.

Principle 6 – Access to personal information

The WCC Issues Resolution Office has a process that supplies and monitors information requests from members of the public and journalists. In the case of the trial, Safe City Living Lab information this could be made available if requested.

Principle 7 – Correction of personal information

No personal information is held so corrections are not envisaged to be necessary.

Principle 8 –Accuracy of personal information to be checked before use

No personal information is collected.

Principle 9 – Agency not to keep personal information for longer than necessary

No personal information is held.

The trial Living Lab CCTV image information is only held on the system while the mapping process occurs, typically less than one minute and is then overwritten as a continuous process.

Principle 10 – Limits on use of personal information

No personal information is held.

The purpose of collecting the information is to inform WCC and other agencies indicated decisions about safety within the Cuba Mall area. Other uses including publication and distribution of the information may be considered on their merits in the future.

Appendix

Information Management Standard

This Standard describes the Council's information management policy, principles and processes. It applies to:

- paper records
- electronic records, and
- information contained within these records.

The information that the Council records contain serves as evidence of activities performed. These records are the essential source of knowledge on how and why decisions were made. Their effective and systematic management is necessary to protect and preserve the information as evidence of action and to support future activities and business decisions.

This Standard covers five main aspects of information management:

- information ownership
- information capture and creation
- information integrity and protection
- information access and use
- information archiving and destruction

Roles and Responsibilities

Staff responsibilities

Role	Responsibilities
Chief Executive, Group Manager Information Management, Manager Risk Assurance	• authorising the Council's Information Management Policy • approving and promoting compliance with this Policy and best practices throughout the Council
Information Management Team Leaders	• the design, building, and maintenance of the Council's File Classification Scheme in consultation with business units • drawing up guidance for best information management practice and its promotion • providing training and support to the Council and employees in the use and interpretation of the Standard • ensuring that the Council's information management procedures support the aims of this Standard • ensuring the integration of information management practice with routine business processes throughout the Council • protecting security-designated information • ensuring that no unauthorised records disposal occurs and all official records approved to be destroyed are disposed of in a manner that protects the confidentiality of the information they contain • ensuring that the Information Management Standard and the guidelines are relevant, current and fulfil the Council's requirements
All group leaders/managers	• ensuring that appropriate information is captured and records are created that clearly represent the business processes and functions in their area • reinforcing the expectation that their employees will comply with the Council's records management policies and procedures • ensuring that all new employees receive an introductory briefing on information management procedures • identifying and selecting information champion(s) within the business unit/team to take responsibility for the management of all current records of the relevant section and liaises with the City Records team • ensuring that appropriate security measures are observed for maintaining official records containing personal or other confidential information

	• assisting with the review of retention requirements when records are due for archiving/destruction • ensuring that employees are adequately trained and supported in the appropriate use of the Standard, procedures and systems
Information Management Staff	• Members of the Information Management Group are responsible for assisting the Team Leaders with their responsibilities, as appropriate, and setting an example to other staff members in information management practice within the Wellington City Council.
All Council employees	• complying with the Council's Information Management Standard • creating full and accurate records of activities, transactions, and decisions carried out during the course of daily business activity • initiating the capturing of the information by the appropriate method • ensuring that electronic records are maintained by being saved into the Council's central electronic document management system or other approved electronic systems relevant to the activity being undertaken • placing papers or other physical records in approved physical file or boxes • handling records with care and respect • preventing unauthorised access to records • ensuring that no records are destroyed or removed unless permitted by a current disposal authority

Information Ownership

Introduction

All information created and maintained by the Council is property of the Council. Employees (permanent or contracted) do not own the information or documents they create while working for the Council. This includes hard-copy files, records on databases and electronic documents.

Establishing ownership

In order to establish ownership of records, the creator must be able to be identified. Employees must therefore ensure all records contain information about their author, title and date of creation.

Custodians of Council records

A custodian is any person or business unit holding information created or received by the Council. Business units/teams may select one person (or more) who is specifically assigned to manage the unit's information, unless it is held in a Council repository managed by City Records. This person is responsible for the storage, security, access, integrity, and maintenance of the records they hold.

The effectiveness of each business unit's custodial management of information is regularly monitored by Risk Assurance and Information Management.

The Council retains the ownership of the information, even when an external party is responsible for managing its records. For example, a database could be managed by an external service provider but the information in the database will be the property of the Council.

If an external party becomes a custodian of the Council's information an agreement must be in place (when the information is transferred) that covers:

- time – when the records will be returned
- protection – what may and may not be done to the records, e.g. they may not be altered or damaged
- access – right to access the information anytime by authorised council employees.

Please contact City Records for further advice.

Copyright

Copyright of external material

The Copyright Act allows 'fair dealing' with 'a work' for the purpose of research or private study. This means you or a librarian on your behalf may copy works for your current project under certain conditions. Employees who have copies of articles or other copyrighted works for the purpose of research or private study may keep those copies as a 'personal reference collection', but may not distribute copies. This also means that if they are kept in the document management system, appropriate security settings need to be applied.

Refer to Copyright Act 1994 - know the rules handout that can be displayed by Council photocopiers.

Copyright on the Council's work

Copyright of all original documents created by the Council belongs to the Council unless a partnership agreement has been made. It is not necessary to place "copyright" or © on each document to protect copyright, however it is strongly recommended that a copyright statement should be printed on all Council publications.

The standard copyright statement used by the Council is:

- *© Wellington City Council (year)*

If you are prepared to allow use of whole or part of the publication, and require only acknowledgement of use, use the following statement:

- *© Wellington City Council (year). Except as authorised by the Copyright Act 1994, the contents of this publication can be used freely with acknowledgement to Wellington City Council*

Where ownership of copyright for published material or intellectual property is shared with an external party this must be included in the copyright statement in the publication.

Contracts with external service deliverers must include a clause identifying the copyright ownership for any published material or intellectual property, if applicable.

Use of the Council's copyright material

In general, individuals, non-profit making organisations, public and charitable organisations may use material or publications produced by the Council free of charge, providing they make no commercial use of the work and acknowledge the copyright.

If a commercial organisation uses the Council's intellectual property in its management or operational activities, the originating business unit may consider

charging them for copyright. In specific cases (eg where the intellectual property is being used in the public good) the originating business unit may agree to waive the copyright fee. In these cases the decision and the agreement must be documented.

Information Capture and Creation

Introduction

Council is required to create and maintain information to document business activities in order to meet operational and accountability requirements. Information must be:

- captured into an official records management system that is approved by Information Management
- complete and have the attributes necessary to function effectively as evidence
- described in a consistent manner in order to aid retrieval and management.

What information to create and capture

Employees must store, or file, any material that documents or supports the administrative, fiscal, legal, and business transactions and functions of the Council. This includes:

- decision papers
- policy papers and recommendations
- reports
- memoranda
- minutes of meetings
- supporting materials, such as substantive drafts, annotated documents, raw data.

Note:

If information is created electronically (this includes scanned documents) it should be stored electronically unless there is a business need to print and file.

For example, paper copies of building consents are currently managed as the record.

Where should the information be stored?

All information must be stored in an approved system. Paper records for example must be kept in official files; electronic records in the appropriate line of business system or approved electronic repository. Employees must follow the standard process associated with the system being used.

Paper files must be located centrally in City Records or within the business unit. When files are moved from their original location, City Records must be notified immediately. Semi-active paper records can be sent to off-site storage managed by City Records.

Mail Register

Some business units maintain a register of all incoming mail and any subsequent action. When setting up a system of mail registration, use the Mail Registration template. The information in all fields must be recorded to make it a usable record.
Refer to Mail Registration template.

Information Integrity and Protection

Introduction

The integrity of a record refers to its being complete and unaltered. A record must be protected against unauthorised alteration. The information belonging to and required by the Council must be protected from:

- destruction or damage caused by environmental factors (eg fire, water, rodents, humidity)
- destruction or loss caused by human factors (unauthorised removal or destruction)
- unauthorised access resulting in unapproved use of the information alteration or corruption, whether intended or unintended

Any authorised annotation, addition or deletion to a record should be explicitly indicated and traceable.
Monitoring and auditing must be done to ensure all security measures are effective.

Disaster recovery

The integrity of the information must be maintained wherever possible during and after recovery from disaster. Every business unit must identify records vital to its

ongoing business and take necessary steps to ensure their protection, currency, and availability during or after a disaster or emergency. This relies on the judgement of the originator of the information, or the users, based on their knowledge of the function of each record. City Records will provide guidance to business units on identifying vital records and recommend appropriate methods for protection.

Storage of records

All paper records must be stored in a way to ensure Council meets its mandatory requirements under the Public Records Act Storage Standard. Physical records must be contained in file covers and boxes approved by City Records.

Business units must have appropriate storage to ensure records are protected, accessible and managed in a cost-effective manner. Refer to City Records for details of approved storage equipment.

Confidential paper records (e.g. personnel files) must be stored in lockable cabinets which can only be accessed by authorised staff. Confidential electronic documents must be stored in restricted access locations where only authorised users have access.

Lending records to others

A business unit must know the location of all its records at all times and be able to identify all those who have had custody of them, for the life of that record.

If a business unit lends records to other units or employees within the Council, it must:

- have a system for tracking those records
- ensure they are protected from unauthorised access.

Records must not leave the Council's premises unless approved by either City Archives or City Records. The appropriate team must be contacted if records are to be taken off the premises.

Closed files

Special rules apply to the use of closed files because of the need to preserve the integrity of the original record. These are:

- nothing must be added to, or removed from, a closed file
- documents on a file must not be marked, annotated or altered in any way.

If you need to add more papers, get the current volume of the file or request a new file from City Records.

Information Access and Use

Introduction

In general all records created in the Council should have open access to other employees and the public. In certain instances however, restrictions may need to be placed on records that are confidential or sensitive in nature.

Restricting access to records

Access to records may be restricted to protect:

- personal information and privacy
- commercial confidentiality
- legal privilege

Restricting access to a record must be for a defined period and not indefinitely. It must be applied only where specifically required by business, or by law.

To place a restriction on the information the business unit manager must be able to justify the grounds for restriction. The following details must be provided to City Records so that the restriction can be implemented:

- which records are to be restricted
- reason for restriction (referring to specific legislation or business requirements)
- who is authorised to access the records, or what permissions are required to access the records
- length of restriction.

Restricted records must be stored in approved records management systems. They must be described discoverable to Council (including who its custodian is) without revealing its sensitive content.

Assigning a security category

Access and security classifications should be assigned to records to indicate the level of restriction or protection required. The Council security categories for current and inactive records are:

- **Personal –** used for an employee's personal files.
- **Private –** used to indicate that a file or record contains information about a member of the public which the Council must keep confidential under the Privacy Act 1993.
- **Commercial –** used to indicate that a file or record contains information which may be restricted by the Council for reasons of commercial sensitivity or legal

privilege, as set out by the Local Government Official Information and Meetings Act 1987 (LGOIMA).

The security classification should be assigned by the business unit, in consultation with City Records, at the time the records are created. If a record does not explicitly state a restricted security category, it is considered to be openly available within Council.

Accessing restricted information

If you need to see a record that is restricted you must get the express permission of the person authorised to release it. In some cases this will need to be written permission.

Borrowing physical records from the City Records or City Archives

The Council employee who borrows records must:

- know at all times where the record is while it is in their custody
- notify Records or Archives staff if they want to pass the record on to another Council employee
- ensure that the record does not leave the Council premises without Records or Archives approval

Access to records by external parties

LGOIMA requires that information held by local authorities be made available to the public unless there is a valid reason not to.

All requests which make specific reference to LGOIMA, however, must follow the procedures outlined in the Information Requests Standard.

Members of the public or external organisations must be supervised as far as is practical when they are given access to original material to deter attempts to tamper with original Council records.

Information, Archiving and Disposal

Introduction

It is important to manage records effectively throughout all stages of their lifecycle. There are three stages of the records:

- current
- non-current (inactive)

- archival

Retention and disposal

The Council has an officially approved retention and disposal schedule, which determines what records, should be retained or disposed of. Business units are required to manage the records they no longer need onsite in accordance with the schedule.

Business units must not destroy records without consultation with City Records or City Archives.

The Council's non-current records will be disposed of in an organised, efficient and, where necessary, confidential way.

Those records required to be retained permanently due to legislative, business or historic reasons, will be transferred to City Archives.

Refer to Records Retention and Disposal Schedule.

Definitions

Appraisal

The process of determining which records are to be retained as archives and which may be destroyed.

Archival value

Qualities possessed by records on account of which they are deemed worthy of permanent preservation for administrative, evidential, legal, financial, historical, cultural or other reasons.

Archives (lower case)

Records which have been assessed to be worthy of permanent preservation for administrative, evidential, legal, financial, historical, cultural or other reasons.

Archives

Is the business unit responsible for the preservation, management and access to the archives? (This term may also be used for the building or repository itself.)

Classification scheme

A logical and systematic arrangement of records into groups which helps enable accurate and efficient retrieval of records

Disposal

The final decision concerning the fate of records, e.g. destruction or transfer to archives.

Document

A piece of written information whether in paper or electronic format including emails, faxes, letters, reports, memos, hand-written notes, spreadsheets.

Electronic records

Information held in electronic format and existing in a system or database, including a document management system or in an unstructured setting such as a folder or email system.

Files

Groups of related documents organised and indexed according to the Council's classification scheme

Inactive records

Records which are no longer required for the conduct of current business and are accessed so infrequently that they can be transferred from offices to separate storage areas.

Information

A collection of data in any form that is maintained by an agency or person and which may be transmitted, manipulated, and stored.

Records
The subset of information that constitutes the evidence of activities.

Records management

The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records.

Records management system

A system in which records are organised and indexed according to the Council's classification scheme. This may be an electronic or a manual system.

Record custodians

Individual employees or business units who hold records and have responsibility for their security, integrity, maintenance and access.

Retention schedule

A set of instructions relating to a class of records, which determine the length of time they should be retained by the Council for business purposes, and the eventual fate of the records on completion of this period of time.

Vital records

Those records crucial to the conduct of an organisation's business, without which an organisation could not continue to operate.