NORTH YORKSHIRE
FIRE & RESCUE AUTHORITY

Records Management Policy

North Yorkshire Fire & Rescue Service
Headquarters
Thurston Road
Northallerton
North Yorkshire
DL6 2ND

Tel: 01609 780 150

www.northyorksfire.gov.uk

Version Control Table

Date of Issue	Version Number	Status
22/09/2016	0.1	First Draft
18/10/2016	0.2	Second Draft
21/11/2016	0.3	Third Draft
15/12/2016	0.4	Fourth Draft
14/02/2017	0.5	Fifth Draft
15/02/2017	0.6	Sixth Draft
02/03/2017	0.7	Seventh Draft
15/03/2017	1.0	First Major Version Publish

Table of Revisions

Date	Section	Revision(s)	Author
22/09/2016	Whole Document	Initial Document	B Eke
18/10/2016	Whole Document	Amendments from CAOMIGO	S Dale
21/11/2016	Whole Document	Amendments to links and content	B Eke
15/12/2016	Whole Document	Amendments from CAOMIGO	S Dale
14/02/2017	Whole Document	Amendments from Head of Finance and Administration	C Godfrey
15/02/2016	Whole Document	Amendments from CAOMIGO	S Dale
02/03/2017	Appendix A	IGG	S Dale
15/03/2017	Whole Document	Corporate Management Board Approval	CMB
13/09/2019	Whole Document	Amendments and full document review by CAOM	J Hawcroft

Contents

1 Introduction

North Yorkshire Fire and Rescue Service (hereafter known as ‘the Service’), recognises that its records are an important corporate asset and effective records management is necessary to support all its business functions. Records justify official actions, decisions and provide evidence required for legal compliance and official audit. This policy will form the basis of a systematic and controlled programme for the management of the Service’s records throughout their lifecycle.

2 Purpose

The purpose of the Records Management Policy is to ensure that full and accurate records of all activities and decisions of the Service are created, managed and retained or disposed of appropriately, in accordance with relevant legislation and good practice.

This policy defines a framework and outlines the responsibilities for effective records management across the Service, ensuring all legal and statutory requirements are met.

3 Scope

A record is defined as information, in any form, created, received, processed, used, maintained, stored, or destroyed by the Service, its elected members, employees, or those acting as its agents in the course of any business activity.

Everyone acting on behalf of the Service must comply with this policy, associated records management standards and procedures in their conduct of business. This policy applies to records in all formats, during their life cycle, from creation until destruction or permanent preservation.

4 Aims of Records Management Systems

The aims of a Records Management System are to ensure that:

- **Records created** – are accurate, authentic and reliable;
- **Records can be accessed** – records and the information within them can be located and displayed in a way consistent with its initial use, and that the current (i.e. most up to date) version is identifiable where multiple versions exist;
- **Records are available when needed** – from which the Service is able to form a reconstruction of activities or events that have taken place;
- **Records history** – the history of the record can be understood: who created or added to the record and when, during which business process, and how the record is related to other records;
- **Records tracking –** systems are to be put in place to enable tracking and location of records;

- **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **Records are secure** – from unauthorised or inadvertent alteration or erasure, whilst access and disclosure are properly controlled and audit trails will track all use and changes. Records are held in a robust format which remains readable for as long as records are required;
- **Records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff are trained** – so that all staff are made aware of their responsibilities for record-keeping and record management.

5 Definitions

Record: A record is recorded information, in any form, including data in systems, produced or received in connection with the Service's work and kept in order to support and/or give evidence of an activity.

Records, if well kept, are a reliable source of evidence and information.

An **evidential record** is a document or piece of information that can be used, to prove that an activity has taken place or explain how a decision or conclusion has been reached. No evidential record should be modified.

Not all the documents and information created, collected or held by the Service will be evidential records and therefore do not need to be kept. and can be routinely destroyed in the normal course of business. These types of record are defined as **'non-evidential'** as they are duplicate, unimportant or only of short-term value, Examples include:

- Catalogues and trade journals;
- Telephone message slips;
- Trivial electronic mail messages or notes that are not related to business activities;
- Requests for stock information such as maps, plans or advertising material;
- Out-of-date distribution lists;
- Superseded stationery and forms (unless controlled);
- Reference copies of annual reports; or
- Working papers that lead to a final report.

Format: A record can be in any format including (but not limited to): paper files, email, audio/visual, electronic documents, systems data, databases, digital images and photographs.

Records management: The control of records during their lifetime, from creation to storage and retention until eventual archival preservation or destruction.

Records creator: The person that produces and receives records and then keeps them in its record keeping system.

Record keeping system: System or procedures by which the records are created, captured, secured, maintained and disposed of.

Records declaration: The process through which records are identified as such and distinguished by other information that is not to be regarded as recorded information.

Official copy: The official copy of a record is the copy intended to give evidence of the activity supported by the record and therefore, if need be, is the one to be submitted to public authorities and other stakeholders and partners.

Convenience copy: A convenience copy of a record is a copy created for the convenience of the records creator or of someone working for the records creator e.g. to give him/her quicker access to the information contained in the record.

Primary responsibility: The primary responsibility over a record identifies which section/person is in charge of keeping the official copy of a record and deciding about specific issues concerning its management.

Vital records: Records without which an organisation would be unable to function, or to prove that a key activity has taken place.

EDRMS: Electronic Documents and Records Management System. The EDRMS may be made up of one or more IT platforms.

Metadata: is information about information. For example, the title and author of a book is metadata. Metadata can be many kinds of information (or columns within a SharePoint Library) — a location, a date, or a catalogue item number. When you use SharePoint products, you can manage the metadata centrally. You can organise the metadata in a way that makes sense in your business and use the metadata to make it easier to find what you want.

Within the Data Protection Act the following terms are defined as:

Data subject means an individual who is the subject of personal data.

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

6 Duties

All staff play a vital role ensuring compliance against the Data Protection Principles and protecting the Service’s information and assets. The key governance roles applicable to records management are;

The Corporate Management Board

The Corporate Management Board (CMB) has ultimate responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

Senior Information Risk Owner

Acting Chief Executive & Monitoring Officer of the OPFCC (Simon Dennis) is appointed as the Senior Information Risk Owner (SIRO) and has overall responsibility for ensuring that information risks are managed accordingly. The Information Controller, Data Controller and Information Technology Security Officer (ITSO) support the SIRO and Information Asset Owners (IAO's) to ensure that risks are identified and managed accordingly, see the flow diagram in Section 14, Policy Governance for further detail on how these roles interact.

Information Governance Group

The Information Governance Group (IGG) act as a discussion forum for issues surrounding the governance of information and the management of records. It provides CMB with the corporate assurance that risks surrounding information, data and associated systems are being managed appropriately. Where necessary it will act as a project or programme board for the implementation of information management or data management systems. Appendix A provides IGG terms of reference.

Central Administration Office Manager

The Central Administration Office Manager (CAOM) is responsible for:

- Raising staff awareness of records management;
- Providing advice and guidance;
- Ensuring compliance with the records management policy and associated standards;
- Maintaining the retention schedule;
- Developing, maintaining and documenting the Service's disposal activity;
- Ensuring that procedures and guidance are in place to support the records management policy.

Information Asset Owners

The Information Asset Owners (IAO) (and delegates) are responsible for information assets in terms of:

- Identifying the assets and risks associated with them;
- Managing and operating the asset in compliance with policies and standards;
- Ensuring their team and those interacting with the asset understand information security and are confident they know how to handle information;
- Ensuring controls manage all risks appropriately; and
- Updating the Information Asset Register.

The **Function Heads** are the named Information Asset Owners (IAO) who take the lead on records management issues within their function and are responsible for the day to day management of the information risks of their assets.

They will;

- Act as a communication point and support the implementation of the corporate records management programme in their respective sections;
- Monitor that their respective sections manage records in accordance with this policy and associated policies, procedures, guidelines and standards;
- Coordinate retention and disposal activities and liaise with the CAO Manager and the Information Governance Group in order to ensure the correct execution of the activities;
- Provide advice and guidance to the staff members of their sections on records management procedures;
- Provide assurance statements to the SIRO regarding the information within their department and;
- Undertake an e-learn IAO training module every two years.

CAO Service Information Team

The CAO Service Information Team (CAOSIT) will:

- Facilitate transfer of non-current paper records to central store;
- Offer prompt and efficient retrieval of paper-based records and controlled access to these records;
- Organise systems to facilitate effective location and retrieval;
- Offer secure, confidential and documented disposal of records in accordance with the Service's records management guidelines;
- Identify vital records and put the necessary procedures in place to protect them.

All Staff

All staff who receive, create, maintain or delete records shall be responsible for ensuring that they do so in accordance with the Service's records management policy, standards and procedures.

External People and Organisations

Contractors, consultants, volunteers, secondees, elected members, partners, suppliers and stakeholders accessing or managing the Service's records shall be responsible for ensuring they do so in accordance with the Service's records management policy, standards and procedures.

External organisations operating as 'Data Processors' on behalf of the Service will be contacted on an annual basis to provide assurances that Service information is being handled in accordance with Data Protection legislation.

7 Records Management

7.1 Elements of Records Management

The Service has formally adopted the principles of the Lord Chancellors Code of Practice on Records Management, issued under section 46 of the Freedom of Information Act 2000 as embodying good practice. The Service recognise that arrangements for managing records may vary, according to statutory or practical requirements and whilst maintaining this flexibility, it is committed to complying with good practice.

Record creation and keeping - Each section should have in place adequate Record Keeping Systems (RKS) (physical and/or electronic) for documenting its activities which take into account the legislative and regulatory environments specific to them. Systems should ensure:

- Accurate, authentic and reliable records are created and kept;
- Records are arranged and indexed in such a way that they can be retrieved quickly and efficiently;
- Procedures are in place for keeping records up to date;
- Metadata is held to enable the understanding of records, support efficient operation of the system and maintain the Service's Publication Scheme;
- Procedures and guidelines are in place for document control, which are easily understood and assist the efficient retrieval of information;
- The ability to cross reference electronic and paper records; and
- Training is provided on how to use the system supported by appropriate documentation.

A list of the Service's main RKS's can be found in Appendix B

Records maintenance and monitoring - Record keeping systems must be maintained in order that records are properly stored, protected whilst being able to be easily located and retrieved. This will include:

- Ensuring records are stored in an environment that provides the requisite levels of security and protection to prevent unauthorised access, damage or loss, whilst allowing maximum accessibility to the information appropriate with its frequency of use;
- Monitoring and controlling the movement and location of records to ensure that they can be easily retrieved at any time, outstanding issues can be dealt with, and an audit trail is held;
- Identifying vital records and applying appropriate protection, including business resilience planning to ensure continued functioning of the Service;
- Identifying records no longer required for the conduct of current business, and if appropriate transferring them to designated storage in line with the retention schedule to optimise the economical and efficient use of office storage; and
- Ensuring electronic and digital records are refreshed, replicated or migrated when new storage devices or media are being installed or when degradation is identified.

Record retention and disposal - With increasing public access to our records, it is important that the disposal or transfer of evidential records is undertaken in accordance with clearly established policies and supported by appropriate documentation. The Service must have in place clearly defined arrangements for the appraisal and selection of records for disposal and enforced by properly authorised officers. This system should ensure that:

- Procedures are in place for the appraisal and disposal (destruction or transfer to an appropriate archive) of records in accordance with the Service's Retention Schedule;
- Disposal activities will be documented and retained in accordance with statutory requirements;
- The destruction of records is undertaken using approved methods appropriate to their protective marking classification;
- Wherever possible, information on the intended disposal of electronic records should be included in the metadata when the record is created;
- Records selected for preservation and no longer in regular use by the Service are transferred as soon as possible to an appropriate archive; and
- Should the Service receive a complaint or appeal about access to information, all records known to be the subject of a request for information will not be destroyed until either disclosure has taken place or, if the Service has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act or appropriate legislation have been exhausted.

Access to The Service's records and information - Records must be available to all authorised employees, their successors and those acting on behalf of the Service that require access for business purposes relevant to the context of their responsibilities. Public access to the Service's records will be in accordance with current legislation. Our Publication Scheme lists the documents and information publicly available and provides information on how they can be obtained from and any related charges. Information not listed in the Publication Scheme or Local Government Transparency Code may be available on request under the relevant legislation. The Service must ensure that any decisions made regarding access to records under the Data Protection Act, Freedom of Information Act or Environmental Information Regulations are documented so that they are consistent and can be explained and referred to.

7.2 Official Copies of Records

There shall be only one official copy of each record. If two records identical to each other need to be kept in order to give evidence of two different processes they shall be considered as two different records, each one associated with its specific features. For example, employee performance reports kept both in the personal record file of the employee and in a grievance file involving the employee.

7.3 Accessing Records

Records shall only be accessed by staff for a business purpose and in line with the Information Security and Handling Policy.

7.4 Storing Records

Records shall be kept in a condition so as to ensure continuing authenticity, accessibility, retrievability, intelligibility and usability throughout their whole lifecycle (including, for those selected for long-term or permanent retention, the period when they are kept in the archives).

7.5 Retention and Disposal

Records shall be associated with its relevant retention schedule. The retention schedule complies with all relevant UK statutory provisions currently in force and will be modified as appropriate.

The retention schedules shall identify the type of record held; the length of time each record is retained; and the way each record is to be disposed of.

Where current legislation does not dictate a retention period, the IAO should decide on the retention duration for their corporate records. Advice should be sought from the CAOM where the IAO is unable to define suitable retention periods.

7.6 Information Asset Owners

IAO's have primary responsibility over the records and therefore are required to authorise a change to the retention or disposal schedule following the expiration of a record if the change is contrary to the original retention schedule.

Legal provisions shall take precedence over proposed modifications.

7.7 Destruction of Records

If provided by the retention schedule, records are to be destroyed when their retention periods expire.

Before destroying any record, it is necessary to verify that there are no specific circumstances that may prevent the destruction, such as legal holds (issued by a Court) or new business needs e.g. the record might be useful to support either legal defence or another corporate activity.

Destruction of records shall be authorised in writing by the relevant manager, or authorised deputy of the function which has primary responsibility over them. The relevant section will ensure all existing copies of the records are destroyed, regardless of format and location.

Destruction of central paper records shall be recorded on the Archive and retention log.

Paper records are to be destroyed by using confidential waste bags or by shredding the record.

Confidential waste bags are to be held and secured at all times to prevent unauthorised access.

Microfiches, microfilms and non-digital photos must be kept separate from paper records and placed in confidential waste bags for destruction.

Electronic records kept within a corporate IT application shall be deleted using the functionality within the application.

7.8 Convenience Copies of Records

Corporate retention and disposal schedules do not apply to convenience copies, which are to be destroyed as soon as they are no longer needed to facilitate the work of the person who has produced them.

8 Record Keeping System (RKS)

There shall be an adequate and appropriate allocation of resources by the Service to maintain its corporate records.

The Service will ensure that records are arranged and identified through the use of a corporate filing system, which also associates them with the relevant retention end date from the Retention Schedule.

The Service will ensure records kept are protected from damaging elements such as water, light, temperature, humidity, fire, infestation, digital viruses, power failures, information leakages and security breaches.

Any off-site storage system shall be considered to be part of the global corporate RKS. Records kept in off-site storage systems shall be managed in compliance with the provisions of this policy.

8.1 Types of Record Keeping Systems

The Intranet, hosted on SharePoint forms the main Electronic Documents and Records Management System (EDRMS). It is used to store, manage and keep most of the Service's digital records. All records should be held on the intranet, unless;

- It is held on another authorised system or database,
- It is incompatible with the intranet and the IAO has authorised it being held on a network drive.

Authorised RKSs used within the Service include:

- FireWatch
- CFRMIS
- Mobilising System – Emergency Incidents
- Incident Recording System (IRS)
- ResourceLink
- Oracle
- ITSS Incident Management System
- Email

Employee's data is also held within the following databases;

- Overtime database for cost analysis purposes
- Fleet plan for standard uniform distribution
- Learn-Pro for e-learn training purposes
- Complywise for health and safety training records
- Ballyclare database maintained by the suppliers of all the Service's operational protective uniform
- Text Database as a communication tool (with consent).

Further information regarding the Service's RKSs can be found in Appendix B.

9 Data Protection

The Service will ensure all records which contain personal data are processed in accordance with the Data Protection Act 2018. Further information can be found within the Data Protection Policy and the Requests made under Data Protection Act (SOP). The main data protection principles are listed in Appendix C.

10 Freedom of Information

The Service will ensure that it complies with its obligations under the FOIA by maintaining a framework for the administration of requests under the Act and subsequent responses. Full information can be found within the following Service Documents:

Freedom of Information and Environmental Regulations Policy

Freedom of Information and Environmental Regulations Procedure (SOP)

11 Information Security

The Service will ensure appropriate security controls are applied to records.

The Information Security and Handling Policy, Protective Security Marking Policy and Information Handling Procedure – SOP is available to all staff to assist with the application of these controls.

In addition, all employees have a responsibility to report any potential, suspected or actual security incident immediately in order that any necessary action can be taken in accordance with the Information Security Incident Management Procedure.

12 Review

This policy and associated procedures will be reviewed every 2 years to ensure they remain up to date and compliant with the law.

13 Further Information

For further information or guidance please contact the Central Administration Office Manager or CAO-SI Team at:

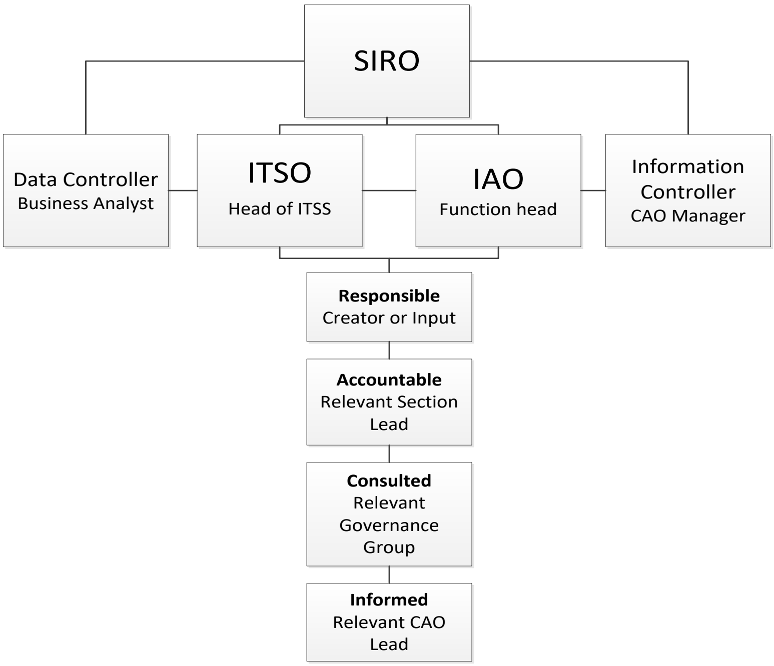
cao.serviceinformation@northyorksfire.gov.uk

14 Policy Governance

A number of identified post holders will be involved in the governance of data to assist the IAO with identifying the information flow, data risks and how to mitigate them. These are:

- **Responsible** – the person/section responsible for capturing the data elements, in this case not necessarily the person entering the data, it is the person requiring the data to be entered.
- **Accountable** – the person accountable for the final decision around the data element, set at section head level.
- **Consulted** – the person consulted before a decision or action is taken around the creation of the data element, set at the appropriate governance group.
- **Informed** – the person informed that a decision or action has been taken (this person may be responsible for the data input, analysis, reporting from the set of data or updating the system accordingly)

These roles play an important part of the information governance arrangements as they have daily interaction with the information assets. The below diagram demonstrates the relationship between these governance roles.



15 Legal and Professional Obligations

The Service will take actions as necessary to comply with the legal and professional obligations in particular:

- The Data Protection Act 2018;
- The Freedom of Information Act 2000;
- Copyright, Designs and Patent Act 1988;
- The Common Law Duty of Confidentiality; and
- any new legislation affecting records management as it arises.

16 Associated Documentation

This policy refers to the following policies and procedures:

- Information Management Strategy
- Freedom of Information and Environmental Regulations Policy
- Retention Schedule
- Data Protection Policy
- Information Security and Handling Policy
- Protective Security Marking Policy
- Information Handling Procedure – SOP
- Information Security Incident Management Procedure.

This policy refers to the following guidance, including national and international standards:

- Section 46 - Lord Chancellor's Code of Practice on the Management of Records

17 Appendices

Appendix A: IGG ToR

INFORMATION GOVERNANCE GROUP

TERMS OF REFERENCE

Purpose of Group

The purpose of the Information Governance Group is to provide corporate assurance that the risks surrounding information, data and associated systems are managed appropriately. Where necessary it will act as a project or programme board for the implementation of information management or data management systems.

Terms of Reference

1. To provide assurance to Corporate Management Board, and the Service where necessary, in respect of the Information Management Strategy including the risk management of information, data and associated systems.

2. To oversee the implementation of any necessary security arrangements in respect if information and data and to provide an organisational link with the regional protective security project.

3. To provide recommendations to Corporate Management Board in respect of resource prioritisation and levels of support required for the implementation and management of information or data management systems.

4. To ensure that information and data management systems are developed in line with organisational objectives and direction.

5. To programme manage the development and implementation of new and existing information and data management systems.

Appendix B: Key Record Keeping Systems Used by the Service

The Intranet
The Intranet, hosted on SharePoint forms the main Electronic Documents and Records Management System (EDRMS). It is used to store, manage and keep most of the Service's digital records. All records should be held on the intranet, unless;

- It is held on another authorised system or database,
- It is incompatible with the intranet and the IAO has authorised it being held on the network drive.

FireWatch
The database processes employees' and previous employee's personal, contractual, sickness, health and safety and training information.

CFRMIS
It's the database to record all fire safety activity which the Service undertakes.

The database processes details of;

- Fire prevention activity, including outcomes from home fire safety visits.
- Fire safety audits of business premises.
- Fire safety audit complaints.
- Site specific risk information.

Mobilising System – Emergency Incidents
The database is used by Control to manage the Service's response to incidents. Incident data is recorded within the database.

Incident Recording System (IRS)
This database is hosted by the Home Office and was introduced for the collection and subsequent statistical handling and publication of incident data from Fire and Rescue Services.

It is used to record details surrounding the incident to identify trends as well as detailing the Service's response.

ResourceLink
The database used by Payroll to process employees pay.

Oracle
The database used by Finance to process trade creditor payments and on occasions used to reimburse employees.

ITSS Incident Management System
The database is used by ITSS to manage helpdesk enquiries.

Standard Test and Asset Register (STAAR)
STAAR is the system used to record the location history and testing records of operational equipment. (The Service is currently trialling AMS as a replacement to STARR)

TRANMAN

TRANMAN is the Fleet Management program used by the Service.

Email
Outlook is used as the email system.

Additional databases
Employee's data is also held within the following databases;

- Overtime database for cost analysis purposes
- Fleet plan for standard uniform distribution
- Learn-Pro for e-learn training purposes
- Complywise for health and safety training records
- Ballyclare database maintained by the suppliers of all the Service's operational protective uniform
- Text Database as a communication tool (with consent).

Appendix C: Data Protection Principles

The eight principles identified in the Data Protection Act 2018 are:

1. Personal data shall be processed **fairly and lawfully** and, in particular, shall not be processed unless –
    - At least one of the conditions in Schedule 2 is met; and
    - In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one of more specified and lawful **purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be **adequate**, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be **accurate** and, where necessary, kept up to date.

5. Personal data processed for any purpose or **purposes** shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the **rights** of data subjects under this Act.

7. **Security.** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country of territory outside the **European Economic Area** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix D: Ten Golden Tips

The tips below will be useful for all staff to ensure The Service's information is handled appropriately.

In the office

1. Never access information unless it is part of your job and you have a business need to do so.

2. Observe a clear desk policy and always 'lock' your computer before leaving your desk.

3. Choose your password carefully and never let anyone else know it.

4. Stop anybody in your building who is not wearing an appropriate security pass and ask to see their ID

5. Always make sure you know what classification the information should have and stick to the rules for that level of protection.

On the move

6. Never take sensitive information out of the office without authority. Never use removable media unless it is business critical to do so and been approved.

7. Keep your laptop, phone and any official papers secure at all times

8. When working outside ensure that you are not overheard and that information cannot be seen by others.

Sharing data

9. Never give out sensitive information over the phone or in any other way unless you are absolutely sure who you are giving it to and that they are entitled to that data.

10. When emailing, ensure you have the correct address for your recipient and that they is a business requirement to share the information with them. Refer to the Information Handling Procedure.