Information Lifecycle and Data Quality Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Information Lifecycle and Data Quality Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd | Jan 18 New Draft |
| 1.1 | Emma Cooper, Kafico Ltd | Jan 2019 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”. |

Contents

[2. Scope 2](#_Toc7420958)

[3. Definitions 2](#_Toc7420959)

[4. Introduction 3](#_Toc7420960)

[5. Statutory Mandatory Framework 3](#_Toc7420961)

[6. Accountable Parties 3](#_Toc7420962)

[7. What Information is Covered? 3](#_Toc7420963)

[8. What is a Record? 4](#_Toc7420964)

[9. Creation 5](#_Toc7420965)

[10. Using / Storage 6](#_Toc7420966)

[11. Retention 7](#_Toc7420967)

[12. Destruction 7](#_Toc7420968)

[13. General Practitioner Records 8](#_Toc7420969)

[14. Change of Contract / Service Provider 8](#_Toc7420970)

[15. National Data Standards 9](#_Toc7420971)

[16. NHS Number 9](#_Toc7420972)

[17. Accuracy and Quality 9](#_Toc7420973)

[18. Information Incidents 10](#_Toc7420974)

[19. Associated Protocols 10](#_Toc7420975)

[20. Audit Schedule 11](#_Toc7420976)

[21. Review 11](#_Toc7420977)

[Appendix A: AoMRC Standards for Medical Records 12](#_Toc7420978)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Suffolk.

At the time of writing and unless alternative protocols have been adopted locally, the protocol applies to;

|  |  |  |
| --- | --- | --- |
| Barrack Lane | Martlesham | Mendlesham |
| Burlington Road | Ravenswood | Wickhambrook |
| Framlingham | Stanton (west) | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | The Birches | Framfield |
| Felixstowe Road | Mount Farm | Saxmundham |
| Hawthorn Drive | Swan and Forest | Guildhall & Barrow |
| The Surgery, Leiston | Glemsford | Peninsula |
| Victoria Surgery | Lakenheath | Little St John Street |
| Ivry Street | Ixworth | Grove Medical Centre |

# Definitions

**Personal Confidential Information** This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

# Introduction

This protocol intends to support staff in recognising records and appropriate management of the records lifecycle and to encourage data quality across the organisation.

# Statutory Mandatory Framework

Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 195811. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format.

Effective records management allows organisations to comply with their legal obligations in respect to transparency and privacy. Being able to locate and rely on records of operations and processing of Personal Confidential Information allows the organisation to be accountable and to operate more effectively.

# Accountable Parties

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure management of the full records management lifecycle and the quality of records held by the Practice. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

# What Information is Covered?

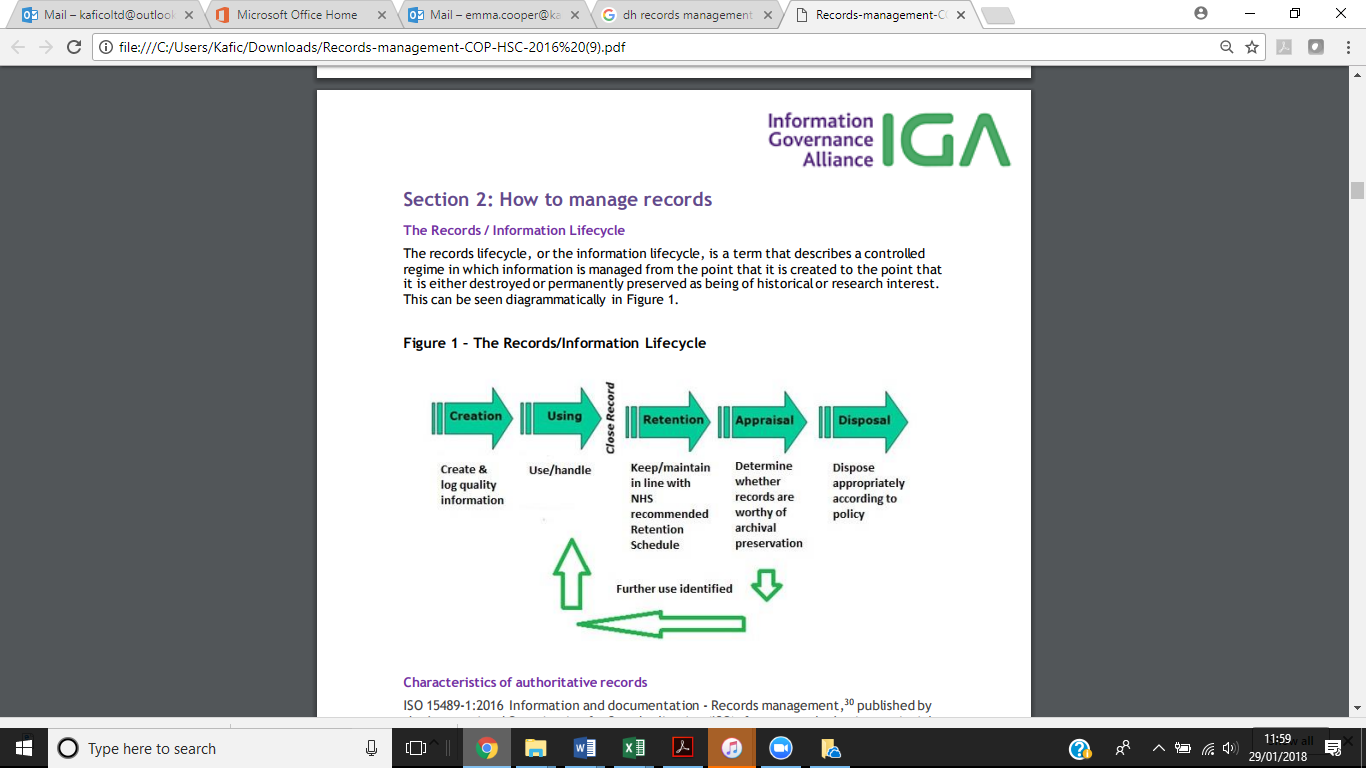
Information is a corporate asset and as such, is an important source of administrative, financial, legal, evidential and historical information; it is vital to the organisation’s future operations, for the purposes of accountability and for an awareness and understanding of its history; information is the corporate memory of the organisation.

Information may be held on paper, USB sticks, computer file or printout, laptops, tablets, mobile phones or even heard by word of mouth or telephone.

This protocol provides general guidance about records management and data quality. When managing medical records, it is also necessary to comply with the standards identified at **Appendix A Standards for Medical Records.**

Without high-standards of information quality, supported by systematic processes and practice, we cannot support the delivery of high quality services and continue to improve.

The diagram below identifies the records management lifecycle and each part of the lifecycle needs to be consistently managed to encourage high standards.



# What is a Record?

A record is information that memorializes and provides evidence of activities performed, events occurred, results achieved, or statements made. Records are created/received by an organisation routinely in the process of its business or in pursuance of its legal obligations.   
Records include accounts, agreements, books, drawings, letters, magnetic/optical disks, memos, micrographics, etc. Generally speaking, ‘records’ function as evidence of activities, whereas ‘documents’ function as evidence of intentions.  
Some activity will be predefined as a record that needs to be kept, such as clinical records. Other records are kept because they are a unique instance of an event such as a business document or email.

# Creation

Records must be created within clinical systems or stored in the shared network

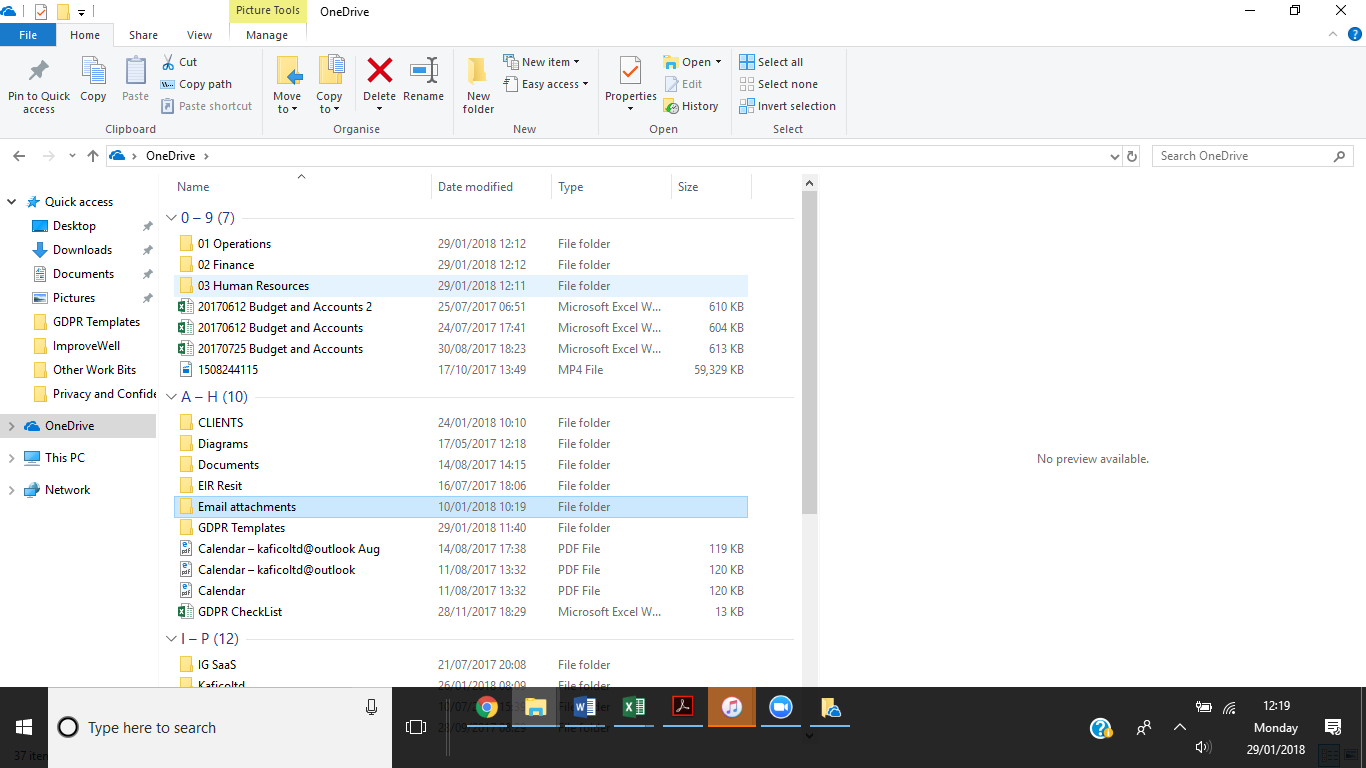
Records must not be stored in personal drives or mobile devices such as mobiles or memory sticks

The filing and naming of records should follow the Function-Activity-Transaction approach.

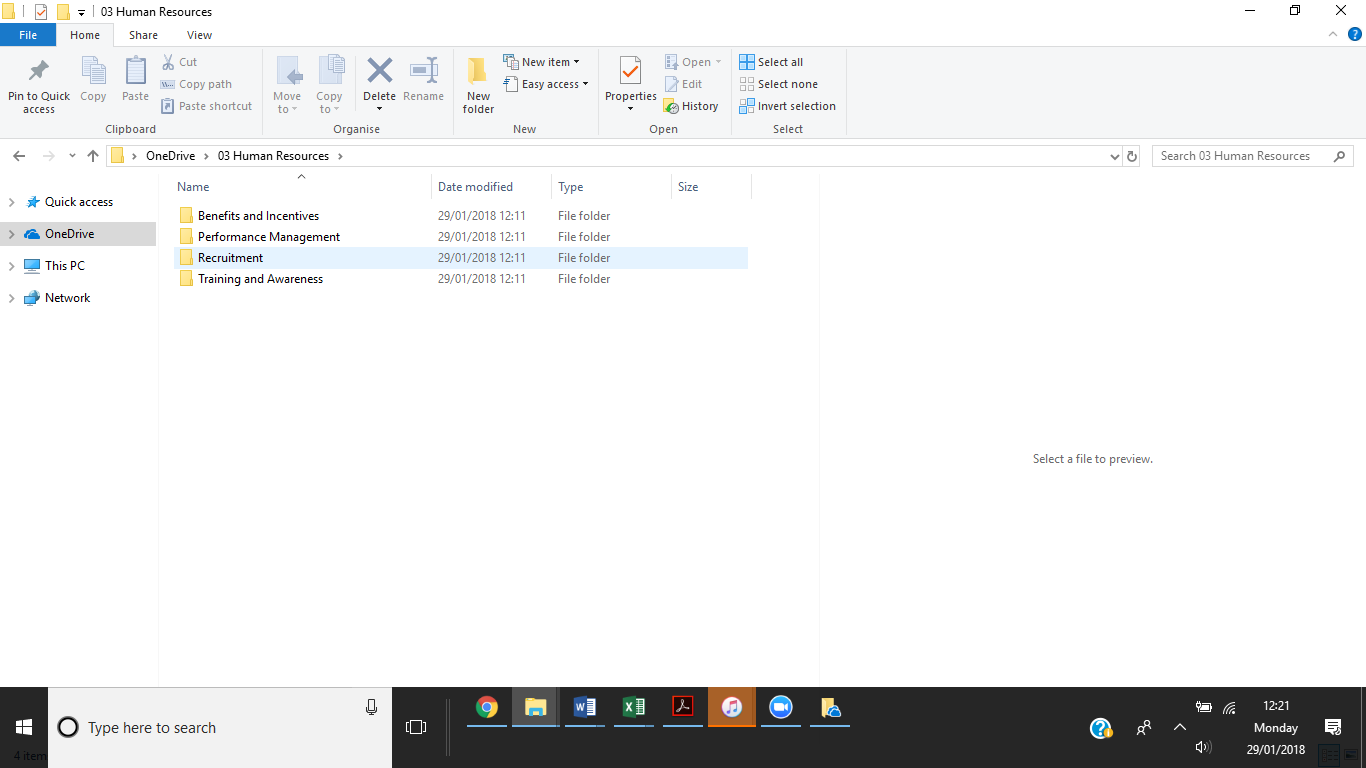
This means that the top-level folder would be named in line with the function, the second level named in line with the activity and the then in line with the transaction.

Example of

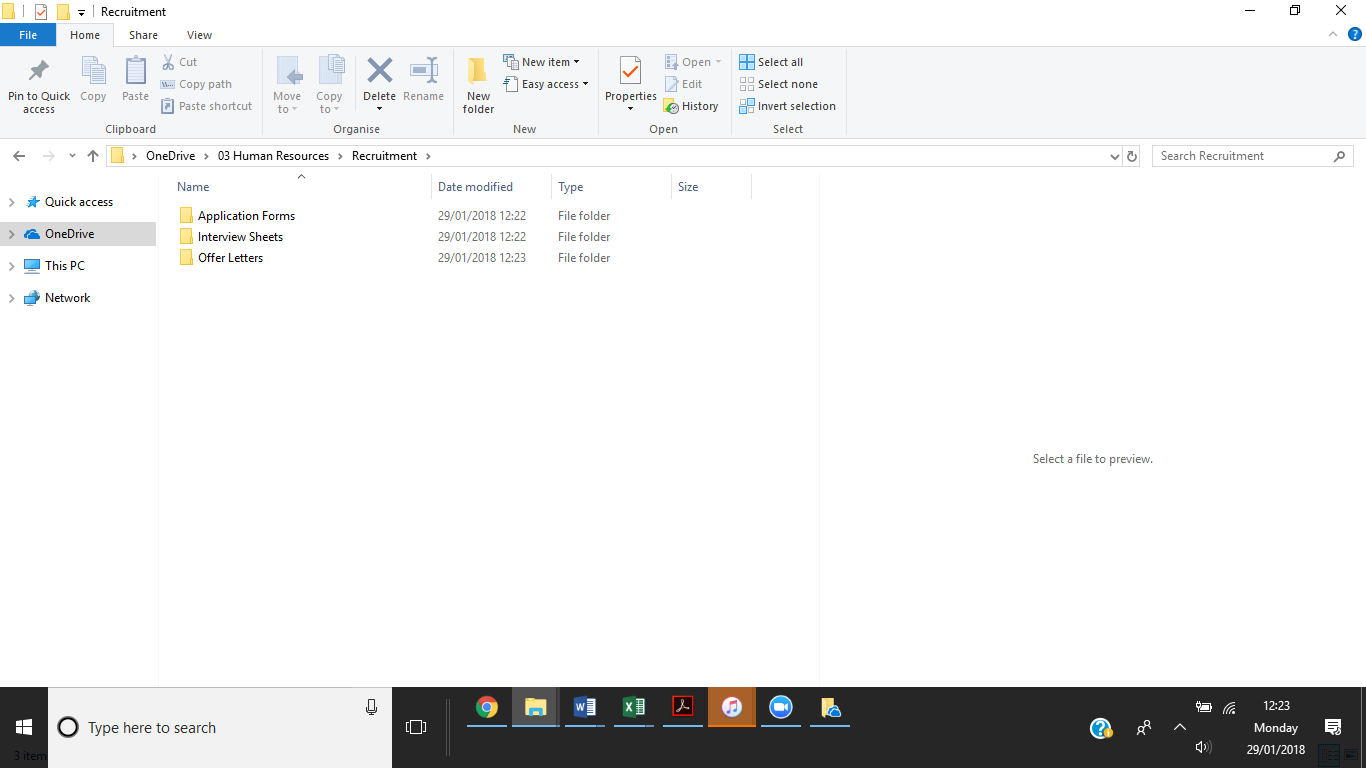
Level 1 – Function – Human Resources



Level 2 – Activity – Recruitment



Level 3 – Transaction – Application Forms / Interview Sheets / Offer Letters



Naming of specific documents should follow a clear consistent method such as including the date of creation or activity, the title and the version.

Example

20180129 Emma Cooper Application Form v1

# Using / Storage

Paper Records

In order to establish the authenticity of paper records and to meet the Care Records Guarantee that the service user can see who has accessed their records, the records must be held in a way that allows The Practice to audit who has accessed it.

Clinical records must be able to be tracked through the entire lifecycle up to destruction, or transfer to the National Archives or an approved place of deposit.

Paper records must be kept in a safe, dry and secure location

**Digital Records**

Digital information must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format

Systems for storing digital records must provide information about those who have accessed the record, as required by the Care Records Guarantee.

When using digital records within a system such as a database or clinical system, you must provide any requested information such as reason for access

When using a digital record being within the shared network such as a Word or Excel document, care must be given to providing ‘metadata’

This will include identifying the author, version, changes made, owner of the document

All information relating to a specific record must be stored together. For example, email messages related to a specific recruitment campaign must be stored in the network Recruitment folder alongside the Application Form and Interview Sheet.

Hyperlinks or embedded documents must still work when the document is transferred to different media or later versions

# Retention

Once a record is no longer being used for its primary purpose, it should be appraised to consider whether and if so, how long, it should be retained by the organisation.

Retaining records for longer than the intended purpose in identifiable form and without an alternative lawful basis is a breach of Data Protection legislation

The Practice uses the Department of Health Records Management Code of Practice to assign retention periods

Staff should have access to a list of key records and their retention periods for that particular department. If you do not have this, please contact the Information Governance Lead or Data Protection Officer

Where the record is being retained, there should be a documented consideration of whether the information could be de-identified (direct or indirect identifiers removed) to reduce the risk of an information breach

# Destruction

Paper Records

Paper records can be incinerated, pulped or shredded (using a cross cut shredder) under confidential conditions.

Do not use the domestic waste or put them on a rubbish tip, because they remain accessible to anyone who finds them.

Staff must keep accurate records of destruction and appraisal decisions. Destruction implies a permanent action.

**Electronic Records**

Destruction of hard assets, like computers and hard drives and backup tapes, must be auditable in respect of the information they hold.

An electronic records management system will retain a metadata stub which will show what has been destroyed.

The Information Commissioners Office has indicated that if information is deleted from a live environment and cannot be readily accessed then this will suffice to remove information for the purposes of the Data Protection Legislation.

# General Practitioner Records

It is important to note that the General Practitioner (GP) record is the primary record of care

The majority of other services must inform the GP through a discharge note or a clinical correspondence that the patient has received care.

This record is to be retained for the life of the patient plus at least ten years after death.

The GP record must transfer with the individual as they change GP throughout their lifetime.

Following the move to digital GP records after the ‘paperlite’ accreditation process there was an instruction not to destroy the paper Lloyd George folders.

The GP2GP programme still requires the Lloyd George paper records to be transferred until further notice

GPs are obliged by their contract to follow the HSCIC, DH and NHS England good practice guidance.

# Change of Contract / Service Provider

When a service provider is changed, the exiting service provider still has a liability for the work they have done and so the records must be retained until the time period for liability has expired.

The commissioner may direct a transfer of care records to a new provider for continuity of upon termination of the contract.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation.

Where the contract change relates to delivery of health and social care, it may be necessary to inform the individuals concerned about the change.

Where there is little impact upon those receiving care, it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes may require individual communications or obtaining explicit consent.

Although the conditions of Data Protection legislation may be satisfied in many cases there is still a duty of confidence which requires a patient or client (in some cases) to agree to the transfer.

If The Practice is adopting a new service, a full inventory of transferring records should be obtained. Likewise, when surrendering a service to a new provider, The Practice should provide an inventory.

# National Data Standards

The use of national data standards should be incorporated were it supports the appropriate sharing, exchange and monitoring of information.

Systems and processes should be evaluated to consider what national data standards are relevant and how they will be incorporated.

Any risks from not using these standards will be considered, recorded and appropriately managed.

# NHS Number

The NHS Number is the unique identifier within the Health Service.

Where available, it must be incorporated into all correspondence with patients and relevant information systems to ensure that the correct individual is identified.

This has been a policy requirement for a number of years, but Health and Social Care (Safety and Quality) Act 2015 provide a further mandate with statutory force; where the requirement can be met, it is a legal requirement to do so.

# Accuracy and Quality

It is understood that errors and inaccuracies will occur in Information.

Systems, process and analysis during the lifecycle of the information need to identify the causes of any errors, the relevant margin of error introduced into any subsequent use of the Information and the appropriate action taken.

This includes understanding the context of any Information or Data Set, to ensure that “outliers”, results that fall outside expected ranges, are investigated to determine if there are any resulting Information Quality concerns.

It is important to determine and maintain a view of expected ranges of information to support the principles of Information Quality.

A Data Protection Impact Assessment should be completed for new processing activities to determine how data quality will be maintained

Information Asset Owners should determine and document the specific data quality measures in place for the Information Asset

Information coming in to the practice must be checked for accuracy and completeness

Where incomplete, they should be returned to the sending organisation and the issues flagged with the appropriate lead

Manual quality checks should be completed on correspondence containing Personal Confidential Information

Systems should have the capacity to run data quality reports to identify duplications or incomplete records

Procurement of systems should include built in measures to maintain data quality such as reduction of free text boxes and the use of drop down lists

Integration with other systems should consider data validation and the potential for errors requiring manual intervention

Data Quality audits must be completed regularly and the results reporting into the Information Governance Lead or Data Protection Officer

Where errors are identified, appropriate mitigation is required. This includes correction, where relevant, analysis of process and appropriate action, and ongoing monitoring.

Understanding the cause of error and its likely consequence are a key component of improving Information Quality or managing issues that cannot be addressed through appropriate controls.

# Information Incidents

Any suspected or actual incidents involving Personal Confidential Information must be reported immediately in line with the Information Incident Protocol.

# Associated Protocols

This policy should be read in conjunction with;

* Risk Management Policy
* Change Management Policy
* Information Governance Policy
* Information Rights and Access Protocol
* Information Sharing and Privacy Protocol
* Information Lifecycle and Data Quality Protocol
* Information / Cyber Security Protocol
* Information Incident Protocol
* Information Risk and Audit Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

# Review

This protocol will be reviewed every year or sooner where necessary

# Appendix A: AoMRC Standards for Medical Records

