Information Governance
Strategic Plan
March 2017 – February 2018

(Requirement to review annually in line with IG Toolkit Standards)
<table>
<thead>
<tr>
<th>Policy Title:</th>
<th>Information Governance Strategic Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Executive Summary:</strong></td>
<td>The Strategic Plan identifies those individuals with responsibilities in the management and safeguarding of information. It sets out the key information governance arrangements and processes and defines the objectives of and responsibility for each of these within the Trust.</td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
<td>Information Governance Strategic Plan v7</td>
</tr>
<tr>
<td><strong>Description of Amendment(s):</strong></td>
<td>The amendments made in this refresh of the Strategic Plan are: Forward – number of people employed by the Trust changed and detail of Caring Together / partnership working added Section 5: Inclusion of information on GDPR and the National Data Guardian role Section 7: New Strategic Workplan for 2017/18 Section 8.1: Inclusion of Chief Executive responsibility being the Identified Section 8.44: Inclusion of role of Caldicott Group Section 8.1: Inclusion of Qualified Person for Freedom of Information requests Appendix 3: Refresh to reflect revised terms of reference for Clinical Management Board; Information Governance; Data Quality; and Records Management Sub-Committee Appendix 3: Inclusion of Caldicott Group terms of reference</td>
</tr>
<tr>
<td><strong>This policy will impact on:</strong></td>
<td>This is a Trust wide Strategic Plan and impacts on all areas.</td>
</tr>
<tr>
<td><strong>Financial Implications:</strong></td>
<td>There are no significant financial implications in the implementation of this Strategic Plan other than audit and training time for all staff, including additional training for those with specific roles that support information risk management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Area:</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document Reference:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Version Number:</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Effective Date:</strong></td>
<td>March 2017</td>
</tr>
<tr>
<td><strong>Issued By:</strong></td>
<td>Head of Integrated Governance</td>
</tr>
<tr>
<td><strong>Review Date:</strong></td>
<td>February 2018</td>
</tr>
<tr>
<td><strong>Author:</strong></td>
<td>Head of Integrated Governance</td>
</tr>
<tr>
<td><strong>Impact Assessment Date:</strong></td>
<td>March 2017</td>
</tr>
</tbody>
</table>

**APPROVAL RECORD**

<table>
<thead>
<tr>
<th>Consultation</th>
<th>Committee Approval</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by:</td>
<td>Clinical Management Board</td>
<td></td>
</tr>
<tr>
<td>Received for information:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director of Corporate Services / Senior Information Risk Owner (SIRO)</td>
<td>January 2017</td>
<td></td>
</tr>
<tr>
<td>Information Governance &amp; Records Management Group</td>
<td>January 2017</td>
<td></td>
</tr>
<tr>
<td>Cascaded via trust-wide policy cascade process. Information Governance Strategic Plan</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Foreword

East Cheshire NHS Trust (the trust) is an integrated community and acute NHS Trust, employing circa 3,000 people. The Trust’s services are managed through three clinical directorates supported by corporate functions. Acute services are managed through a payment by results contract and Community Services a block contract.

The Trust is a partner of the Caring Together programme, which aims to deliver a new integrated care system for the local population.

The Trust needs to ensure that the organisational arrangements for information governance are fit for purpose and that there are robust systems and processes in place. This will enable the Board to fully discharge its duties and overall corporate accountability for the Trust’s strategies, policies and actions.

Information governance forms part of the Trust’s integrated governance approach, which will ensure that credible information is available to support the Trust’s objectives and the principles of corporate and clinical accountability. An important part of integrated governance is quality therefore any information must be able to stand up to public scrutiny.

Information governance allows organisations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively to provide the best possible care.

John Wilbraham
Chief Executive

Julie Green
Director of Corporate Affairs and Governance

Senior Information Risk Owner
Table of Contents

1. Introduction .................................................. Page 5
2. Aims .................................................................. Page 5
3. The Trust Board’s Intent ................................. Page 5
4. Scope ................................................................ Page 6
5. General Principles ............................................ Page 6
6. Information Governance Toolkit ................. Page 8
7. Strategic Work plan .......................................... Page 9
8. Accountabilities, Responsibilities and Organisational Framework Page 10
9. Information Governance Incidents & Reporting Page 13
10. Systems for Monitoring the Effectiveness of the Strategic Plan Page 13
11. Measuring Performance and Review ............. Page 13
12. Implementation, Training and Support .......... Page 14
14. Other Relevant Policies ................................. Page 14

Appendix 1 Definitions ...........................................
Appendix 2 Additional Information roles and Responsibilities
Appendix 3 Terms of Reference for Information Governance Committees/ Group
Appendix 4 Strategy for Clinical Involvement in Activity Recording and Coding
Appendix 5 Acronyms .............................................
1. Introduction

Information Governance is about the way in which the organisation handles its business and personal data. The organisation relies on good quality information being available at the point of need in order to provide a quality service. Staff need to have confidence in the quality of data they use to make decisions about patient care and treatment and the way in which we use resources and run our business. They should understand their own responsibility for recording information to a consistently high standard and for keeping it secure and confidential. Public confidence in our ability to handle their data responsibly and efficiently is based on a good reputation for keeping their data safe and from their own personal experience when using our services.

Information Governance allows organisations and individuals to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care. It applies to all information management activity in its broadest sense and underpins both clinical and corporate governance.

This Strategic Plan identifies those individuals with responsibilities in the management of information across the organisation. It sets out the key structures and processes and defines the objectives of and responsibility for each of these within the Trust.

2. Aims

This Strategic Plan provides the framework within which the Trust will ensure that information is appropriately and effectively managed, properly controlled, is accessible and available for use. It links key policies together and provides a corporate structure within which to assess and address information governance requirements.

The key aims of the Strategic Plan will be to:

- ensure confidentiality where appropriate and support the provision of high quality care by promoting the effective and efficient use of information
- encourage a change in the way individuals think and act, thus developing responsible staff who work closely together, preventing duplication of effort and enabling more efficient use of resources
- develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- enable the organisation to understand its own performance and manage improvement in a systematic and effective way

3. The Trust Board’s Intent

The East Cheshire NHS Trust Board is committed to leading the organisation forward to deliver a quality service and achieve excellent results, thereby ensuring that the organisation delivers the best care possible, is the right place and makes the very best possible use of public funds. The Board intends to use the information governance processes outlined in this Strategic Plan as a means to help achieve this.

The objective of the Information Governance Strategic Plan is to create a culture that encourages staff to manage, handle and safeguard information held in line with legislation and local requirements.
Strategic Objectives

The following are the strategic objectives which have been agreed by the Trust Board.

<table>
<thead>
<tr>
<th>PATIENTS</th>
<th>PEOPLE</th>
<th>PARTNERSHIPS</th>
<th>RESOURCES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide safe, effective personal care in the right place</td>
<td>Build, value and develop a motivated and sustainable workforce</td>
<td>Work within the Caring Together framework to deliver our vision</td>
<td>To deliver services that are clinically and financially sustainable</td>
</tr>
</tbody>
</table>

This Information Governance Strategic Plan is one of the components which support the Board’s objective to Trust’s objective to provide safe, effective personal care in the right place, which encompasses the maintenance of compliance with regulatory authorities for the protection of patients.

See Appendix 1 for Definitions used within this plan

4. Scope

This Strategic Plan is intended for use by all directly employed, agency staff and contractors engaged on East Cheshire NHS Trust business who have been authorised to access and use Trust information and/or systems.

All Information Systems within the Trust (both electronic and paper based) fall within the scope of this framework. Main information systems include Patient Information Systems, Finance, Human Resources, Integrated Risk Management and Payroll databases.

All information and data collected or accessed in relation to any Trust activity whether by Trust employees or individuals and organisations under a contractual relationship with the Trust. All information stored on facilities owned or managed by the Trust or on behalf of the Trust. All such information belongs to the Trust unless proven otherwise.

5. General Principles

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and security arrangements to safeguard both personal and commercially sensitive information. The Trust also recognises the need to share information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.
The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. It is, therefore, the responsibility of all clinicians, managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

Information governance is concerned with the standards that should apply when information is processed. Information processing has five broad aspects. These encompass how information is held, obtained, recorded, used and shared.

Information Governance provides a way for employees to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Human Rights Act article 8.

The Trust will comply with relevant legislation, codes of practice and guidance.

The Trust will make available non-confidential information about the organisation and its services to the public through a variety of media and will have clear procedures for liaison with the press.

The Trust will give patients ready access to information relating to their own care and will have clear procedures for handling queries from the patients and public.

The Trust will ensure that it has an adequate governance framework to support the information governance agenda, including a comprehensive policy framework, Strategic Plan and improvement plans and staff with appropriate skills.

The Trust will ensure that staff awareness and competence in relation to information governance will be appropriately developed through induction and training.

The Trust will put in place adequate measures for information quality assurance. These will include robust policies and procedures for data collection and clinical and corporate records management, identification and resolution of errors and audits of data quality. The Trust will ensure adequate governance of clinical coding to support Payment by Results.

The Trust will ensure the secure management of its information systems including appropriate asset registers, access control measures, business continuity plans and risk management processes. The Trust will work towards compliance with ISO/IEC 17799: 2005, the international standard for information systems security.
General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). The GDPR will apply in the UK from 25 May 2018.

- The GDPR applies to ‘controllers’ and ‘processors’. The definitions are broadly the same as under the DPA – ie the controller says how and why personal data is processed and the processor acts on the controller’s behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The Information Commissioners Office have produced a guidance document entitled Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now, which sets out the steps to be taken by organisations to ensure that they are ready for implementation of GDPR.

National Data Guardian

The NHS has introduced a new role of The National Data Guardian (NDG). The purpose of this role is to advise and challenge the health and care system to help ensure that citizens’ confidential information is safeguarded securely, used properly and allows individuals to opt out of information sharing.

6. Information Governance Toolkit

The national Information Governance Toolkit is a framework and dynamic tool provided by the Health and Social Care Information Centre (HSCIC) which allows an organisation to assess itself against a number of requirements and develop and implement an action plan to improve performance. In association with guidance, strategies and codes of practice from the NHS it forms an essential element of the drive to improve information governance and it is the basis of evaluation of the performance of an organisation in this area.

The toolkit takes a holistic approach in relation to management, systems processes and people and is organised into a number of initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Clinical Information Assurance
- Corporate Information Assurance
- Information Security Assurance
• Secondary Use Assurance*

*The primary use for a clinical record is to support the delivery of healthcare to a patient. Secondary uses include supporting payment for clinical care and analysis of Trust performance such as length of stay or day surgery activity. All Trusts are required to send summary records of care to the Secondary Uses Service (SUS).

The Trust is required to submit IG performance reports to the Department of Health, which can be tracked by the Trust Development Authority, Commissioners and other monitoring bodies.

• 31st July baseline self-assessment report
• 31st October 1st self-assessment or “improvement” report
• 31st March Final annual self-assessment report

The final performance assessment is submitted to HSCIC on the 31st March each year and shared with the Care Quality Commission’s National Information Governance Committee. The results are also published on the HSCIC website and made available to the general public.
## 7. Strategic Work Plan 2017-2018

To be read in conjunction with the roles and responsibilities section and associated Terms of Reference.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Requirement / Plan</th>
<th>Monitoring / Assessment</th>
<th>Lead / Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To ensure that Information Governance principles are embedded across all areas of the Trust</strong></td>
<td>Policies / procedures reflect current requirements and are cascaded to all areas of the Trust</td>
<td>All IG related policies are reviewed and approved by Information Governance &amp; Records management Group. Policy Governance report to SQS shows review and cascade of policies.</td>
<td>Head of Integrated Governance March 2018</td>
</tr>
<tr>
<td><strong>To ensure the Trust is ready for the introduction of GDPR in 2018</strong></td>
<td>Review, assess and implement the 12 step plan for implementation of GDPR</td>
<td>Regular progress updates to the IGRM group.</td>
<td>Head of Integrated Governance March 2018</td>
</tr>
<tr>
<td><strong>Systems and Processes are sufficient to ensure the safeguarding of information assets</strong></td>
<td>System summaries and business continuity plans are in place for all critical systems. Systems and controls have been identified in the Information Asset Register and are regularly reviewed.</td>
<td>Feedback from Critical Systems group to Information Governance &amp; records Management Group. Bi-annual report to Information Governance &amp; Records Management Group.</td>
<td>Integrated Governance Manager December 2017</td>
</tr>
<tr>
<td><strong>To ensure robust processes are in place to safeguard the Trust against cyber attacks.</strong></td>
<td>To enhance reporting processes with regard to cyber security and raise awareness through IG Training sessions.</td>
<td>Routine reporting to SIRO and regular update to IGRM Amended IG Training material.</td>
<td>Integrated Governance Manager October 2017</td>
</tr>
<tr>
<td><strong>All information shared with other organisations is done so on a legal basis having regard for the Data Protection Act</strong></td>
<td>Develop use of the Information Sharing Gateway Continue to work with Directorates to ensure discussions take place early in the process, with sufficient time to allow an agreement to be put in place.</td>
<td>Information Sharing Agreement report to Information Governance &amp; Records Management Sub-Committee</td>
<td>Integrated Governance Manager December 2017</td>
</tr>
</tbody>
</table>
To ensure that retention and disposal of information is in line with Department of Health’s Code of Practice for Records Management

Review the existing archiving arrangement with Deepstore.
Continue to check unknown content boxes currently in storage and destroy as appropriate
Meet with Deepstore representative to review agreement content.
Visit to Deepstore premises and report back to Information Governance & Records Management Group.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Requirement / Plan</th>
<th>Monitoring / Assessment</th>
<th>Lead / Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 95% staff complete mandatory modules within the HSCIC Information Governance Training Resource</td>
<td>Roll out the revised IG Training modules when available. Ensure compliance across the Trust</td>
<td>Cascade new training requirements across the Trust, as and when available. Training performance reports from ESR to be provided to Associate Directors on at least a monthly basis</td>
<td>Integrated Governance Manager January 2018</td>
</tr>
<tr>
<td>Information Governance incidents are kept to a minimum</td>
<td>Review of all information governance / data protection incidents and development of action plans / learning. Investigate all instances requiring reporting to the Information Commissioners Office.</td>
<td>Review of incident category reports / trend analysis/ learning and corrective measures by Caldicott Group Review of RCA by SIRO / Deputy SIRO</td>
<td>Head of Integrated Governance February 2018</td>
</tr>
<tr>
<td>Maintain Information Governance Toolkit level 2 and progress towards level 3 for identified requirements</td>
<td>Identify and collect evidence to support compliance with Level 2 the revised Information Governance Toolkit requirements</td>
<td>Regular reporting to Information Governance &amp; Records Management Group</td>
<td>Head of Integrated Governance and Integrated Governance Manager March 2018</td>
</tr>
</tbody>
</table>

8. Accountabilities, Responsibilities and Organisational Framework
8.1 Information Governance Structure

Effective leadership is essential to create and nurture a culture conducive to information governance. Developing the correct culture is essential as it will mean for example, that data is entered “right first time” and “at the right time”. Commitment from the top is crucial and East Cheshire has a Senior Information Risk Owner (Director of Corporate Affairs and Governance) and the Caldicott Guardian (Associate Medical Director – Clinical Effectiveness) both are supported by deputies.
The following managers have particular responsibilities in respect of information governance, as summarised below and within Appendix 2.

<table>
<thead>
<tr>
<th>Role</th>
<th>Information Governance area</th>
</tr>
</thead>
</table>
| Chief Executive                                           | Overall accountability for Information Governance (delegates responsibility to Director of Corporate Affairs & Governance).  
|                                                            | Is also the Identified Qualified Person for Freedom of Information requests                  |
| Director of Corporate Affairs and Governance              | Responsible Executive Director for Information Governance. Senior Information Risk Owner (SIRO) |
| Associate Medical Director - Clinical Effectiveness       | Caldicott Guardian - delegated responsibility from the Medical Director for the governance of patient information (including information sharing and protection of patient data). |
| Deputy Director of Corporate Affairs and Governance       | Deputy Director of Corporate Affairs and Governance is responsible for ensuring that systems and processes are in place to ensure sound information governance across the Trust. To act as the Deputy Senior Information Risk Owner. Responsible for review and oversight of IG Strategic Plan. |
| Clinical Director for Dental Services                     | Will act as the Deputy Caldicott Guardian                                                   |
| Head of Integrated Governance                            | Data Protection Officer for the Trust and management responsibility for the Information Governance function.  
<p>|                                                            | Operationalises the Data Protection Policy and promotes data protection awareness throughout the organisation |
|                                                            | Completion and submission of the annual information governance assessment. Support and professional advice to the Caldicott Guardian. |
|                                                            | Co-ordination, implementation and monitoring of the information governance Strategic Plan.    |
| Integrated Governance Manager                            | Supports the Data Protection Officer, Caldicott Guardian and SIRO in ensuring that the organisation complies with the Data Protection Act 1998. Reviews reported incidents and ensures that appropriate action is taken. Has responsibility for ensuring that policies and procedures relating to the IG function are adequate and up to date. |
| Chief Clinical Information Officer, Consultant in Emergency | Responsible for the provision of advice and support around the adoption of information governance principles within clinical information systems |
| Information Governance Officer                           | Supports delivery of Trust wide systems and processes to support effective risk management of the information governance agenda and compliance. Maintains the Trust’s portfolio of evidence within the IG Toolkit. |
| Information Security Manager                             | Part of North West Commissioning Support Unit. Responsible for providing advice and support on all aspects of information security including security of information systems, business continuity and system access |</p>
<table>
<thead>
<tr>
<th>Role</th>
<th>Information Governance area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of Communications Engagement and Marketing</td>
<td>Manages Freedom of Information function and ensures the Publication Scheme is maintained.</td>
</tr>
<tr>
<td>Head of Information</td>
<td>Has overall responsibility for the operational management of data quality and for ensuring that clinical staff are engaged with data quality issues, including coding review and validation.</td>
</tr>
<tr>
<td>Legal Services Manager</td>
<td>Responsible for Subject Access function and acts as Freedom of Information Appeals Officer.</td>
</tr>
<tr>
<td>Out Patient Services Manager</td>
<td>Responsible for the health records library function.</td>
</tr>
</tbody>
</table>

**8.2 Managers, Supervisors and Other Staff**

Managers, Supervisors and Staff will be responsible for ensuring the local implementation of this Strategic Plan and that they implement the appropriate information policy within their sphere of responsibility. This includes. Clear accountability arrangements will ensure that staff are held to account for the work that they do and this will be reinforced through contractual arrangements.

All staff will:

- Comply with the Information Governance Strategic Plan and relevant policies
- Be responsible for attending mandatory training including all relevant Connecting for Health Information Governance Toolkit training modules
- take appropriate management action should non-compliance with policies arise

**8.3 Contractors**

It is the responsibility of each contractor employed by East Cheshire NHS Trust to ensure that any staff working on their behalf are fully conversant with the Trust Policies in respect of the activity for which they are engaged.

**8.4 Committee Structure**

See Appendix 3 for Terms of Reference

**8.41 Clinical Management Board**

This Board is accountable to the Trust Board via the Chief Executive who is the Chair of the Clinical Management Board and is attended by Executive Directors, and Clinical Directors.

- The Clinical Management Board will provide assurance that management plans are in place to deliver the Board objectives and will ensure clinical engagement exists at the highest level of operational decision making by:
  - Monitoring performance against key objectives
  - Ensuring strategic and corporate risks are being actively managed
- To shape annual and strategic plans to secure foundation trust status
- Resolve operational issues that impact across the Trust
- To ensure there is clear linkage with Business Groups and other Corporate Functions

The Information Governance and Records Management Group reports to the Clinical Management Board.
8.42 Information Governance and Records Management Group

The Information Governance and Records Management Committee reports to the Clinical Management Board and is chaired by the Director of Corporate Affairs & Governance (SIRO). Its role is:

- To provide a framework to ensure that all clinical and non-clinical information is managed legally, securely, efficiently and effectively. To provide regular reports to Clinical Management Board and highlight progress with IG Toolkit compliance and escalate any areas of concern.
- To ensure full compliance with both legal and best practice requirements: HSCIC Information Governance Toolkit, Care Quality Commission Standards, professional bodies and Royal Colleges.

8.43 Health Records Management Sub-group

The Health Records Management Sub-group reports to the Information Governance and Records Management Group and is chaired by the Caldicott Guardian. Its role is to review:

- To assist the Information Governance and Records Management Group in Trust-wide co-ordination and prioritisation of all health record management issues.
- To make recommendations to the Information Governance and Records Management Group for improvements in relation to policy and/or practice relating to records management.
- To review operational issues relating to health records management as delegated by Information Governance and Records Management Group including assistance to Information Governance and Records Management Group in its function to ensure full compliance with both legal and best practice requirements: HSCIC Information Governance Toolkit, Care Quality Commission Standards, Department of Health Records Management Code of Practice

8.44 Caldicott Group

The Caldicott Group has been established as a sub group of the Information Governance & Records Management Group. Its role is to:

- To identify outstanding Caldicott issues.
- To provide assurance that all actions necessary, in relation to Caldicott issues, have been taken and in accordance with the Caldicott Report (1997) and the guidance and recommendations contained within.

8.45 Data Quality Steering Sub Group

The Data Quality Steering Sub group reports to the Information Governance and Records Management Group and is chaired by the Principal Information Analyst. Its role is to review:

- Information Data Flows for quality, identifying any potential issues
- To ensure up to date systems and process documentation is available for all staff to ensure accurate and consistent information gathering
- To highlight to the Trust any potential issues with regard to quality of data/information collection

See Appendix 4 for Strategy for Clinical Involvement in Activity Recording and Coding
9. Information Governance Incidents and Reporting

There should be a supportive environment within the organisation that is committed to learning from mistakes and sharing that learning. All incidents indicating a suspected or actual information security breach should be reported, according to the Information Security Policy, to the immediate line manager in the first instance and an incident report completed on DATIX.

East Cheshire Trust operates a standard incident reporting process, using the DATIX electronic Integrated Risk Management system, which is used for the reporting of all incidents including those relating to Information Governance. The Information Governance Policy and Policy for the Management and Investigation of Incidents contains further information on incident reporting. Serious incidents (level 2) are reported externally via the HSCIC Incident Reporting Tool.

10. Systems for Monitoring the Effectiveness of the Strategy

Information Governance and Records Management Group will have a rolling work programme that reflects all aspects of information governance.

Twice yearly assurance reports will be provided for review by the Clinical Management Board.

An Annual Governance Statement, which includes risk management in East Cheshire NHS Trust based on all available relevant information, will be produced by the Director of Corporate Affairs and Governance. This report, together with performance against the Key Performance Indicators, will be reviewed by the Trust Board.

11. Measuring Performance and Review

This Strategic Plan will be reviewed annually by the Information Governance and Records Management Group. Performance will be measured by the IG Toolkit achievement scores and outcomes of both internal and independent audits.

12. Implementation, Training and Support

The effective implementation of this Information Governance Strategic Plan will facilitate the delivery of a quality service and, alongside staff training and support in line with the Trust Training Needs Analysis, Mandatory Training Programme and HSCIC Information Governance Toolkit, will provide an improved awareness of the measures needed to manage, properly control and access information.

East Cheshire NHS Trust will:

- ensure all staff and stakeholders have access to the Information Governance Strategic Plan and Risk Management Strategy;
- develop policies, procedures and guidelines to assist in the implementation of this Strategic Plan;
- Ensure that information governance training is included within the trust training needs analysis
• Ensure all Board Members, Directors, Senior Managers and Staff receive information governance training commensurate with their roles and responsibilities in line with the training needs analysis;
• Ensure attendance at training sessions is recorded onto the electronic staff record and a system employed to ensure that non-attendance is followed up;
• ensure that staff have the knowledge, skills, support and access to expert advice necessary to implement the policies, procedures and guidelines associated with this Strategic Plan; and
• monitor and review the performance of the Trust in relation to the management of information.
13. **Equality Impact Assessment**

This Strategic Plan has been impact assessed with regards to dignity, equality and diversity and there are no areas in the Strategic Plan that contravene equality and diversity guidance. Available via Trust Publication Scheme.

14. **Other Relevant Policies**

All documents in the East Cheshire Policies Schedule are relevant, in particular the following policies will be approved by the Information Governance & Records Management Sub-Committee, who will also seek assurance on compliance with the key indicators within:

- Information Governance Policy
- Information Security Policy (incorporating Internet Usage Policy)
- Records Management Policy
- Email Policy
- Data Quality Policy
- Information Risk Management Policy
- Freedom of Information Policy
- Learning and Development Policy
- Network Security Policy
- Policy for the Management and Investigation of Incidents
APPENDIX 1 - Definitions

Data Controller:

The person or organisation that collects personal data and decides on how to use, store or distribute that data

Data Processor:

Any person or organisation (other than an employee of the data controller) that processes the data on behalf of the data controller

Data Subject:

An individual who is the subject of the personal data

Personal Data:

Data that relates to a living individual that can identify the individual from this data or other information in the possession of the data controller

Sensitive Personal Data:

Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions
Appendix 2 – Additional Information Roles and Responsibilities

**SENIOR INFORMATION RISK OWNER**

**Responsible to:** Chief Executive

**JOB SUMMARY**

The Senior Information Risk Owner (SIRO) is an Executive Director Board Member who will take overall ownership of the Organisation’s Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation’s Statement of Internal Control in regard to information risk.

The SIRO is expected to understand how the strategic business goals of the Organisation and how other NHS Organisations’ business goals may be impacted by information risks, and how those risks may be managed.

The SIRO will implement and lead the NHS Information Governance (IG) risk assessment and management processes within the Organisation and advise the Board on the effectiveness of information risk management across the Organisation.

The SIRO shall receive training as necessary to ensure they remain effective in their role as Senior Information Risk Owner.

**KEY RELATIONSHIPS**

Within the Organisation:

- Chief Executive and other Board members
- Chief Information Officer
- Clinical Management Board
- Deputy Director of Corporate Affairs and Governance
- Chief Clinical Information Officer, Consultant in Emergency
- Head of Integrated Governance
- Integrated Governance Manager
- Information Asset Owners
- Risk Managers
- Information Security Manager
- Programme Managers, Technical Architects
- Records Manager
- Caldicott Guardian, although ownership of the Information Risk Policy and risk assessment processes will remain with the SIRO.

Regularly has contact with:

- Chief Executives, other Senior Information Risk Owners, Caldicott Guardians and Information Governance Leads in other NHS Organisations
KEY RESPONSIBILITIES

1. Policy and process
   - Oversee the development of an Information Risk Policy. This should include a Strategy for implementing the policy within the existing Information Governance Assurance Framework and be compliant with NHS IG policy, standards and methods.
   - Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the Annual Governance Statement.
   - Ensure that the Board and the Accountable Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.
   - Review and agree actions in respect of identified information risks.
   - Ensure that the Organisation’s approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
   - Provide a focal point for the escalation, resolution and/or discussion of information risk issues.
   - Ensure that an effective infrastructure is in place to support the role by developing a simple Information Assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities

2. Incident Management
   - Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements.
   - To ensure that there are effective mechanisms in place for reporting and managing Serious Incidents Requiring Investigation (SIRIs) relating to the information of the Organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.

3. Leadership
   - Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.
   - Advise the Board on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising etc

TRAINING
The SIRO will be required to undertake information governance training in line with the trust’s training needs analysis to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

INFORMATION ASSET OWNER

Responsible to: Senior Information Risk Owner / Line Manager

JOB SUMMARY
The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets within the service/Trust. IAOs will work closely with other IAOs of the
Trust to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities, especially where information assets are shared by multiple services. IAOs will support the SIRO in their overall information risk management function as defined in Trust policy. The IAO will also undertake the role of Data Custodian, as required by the Data Protection Act 1998. The IAO will document, understand and monitor:

• What information assets are held, and for what purpose
• How information is created, amended or added to over time
• Who has access to the information and why
• Understand and address the risk to the asset, providing assurance to the SIRO

KEY RESPONSIBILITIES
1. Identify and document the scope and importance of all information assets they own. This will include identifying all information necessary in order to respond to incidents or recover from a disaster affecting the information asset.

2. Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks.

3. Provide support to the SIRO to maintain their awareness of the risks to all information assets that are owned by the Trust, and for report those risks as appropriate.

4. Ensure that staff and relevant others are aware of and comply with expected information governance and Data Protection working practices for the effective use of information assets:

   • Promote Data Protection & Caldicott Principles on an on-going basis, including distributing posters, communicating articles and giving local briefings.
   • Promote local induction and ensure that all new starters, before they access any information system, are given instruction on the Data Protection Act and Caldicott, as part of their first day/week induction programme.
   • Ensure that all new staff attend the Corporate Induction session as soon as they are able.
   • Ensure that all staff have access to current information on Data Protection Act and Caldicott requirements.
   • Ensure that all staff are aware of the Data Custodian/IAO for their area and the contact details for the relevant Information Security Team.
   • Ensure that all staff know the procedure for reporting information and IT security incidents

5. Provide a focal point for the resolution and/or discussion of risk issues affecting their information assets

6. Ensure that the Organisation’s requirements for information incident identification, reporting, management and response apply to the information assets they own; including ensuring completion of Data Flow Mapping exercises when required.

7. To ensure (via IAA) that the service’s RA Sponsors and Agents list is regularly reviewed and up dated – reporting to the RA Co-Ordinator as appropriate.

8. To undertake information risk management training as required to ensure skills, capabilities, and any new national requirements are kept up to date.

9. To supervise and delegate tasks to the Information Asset Administrator.
INFORMATION ASSET ADMINISTRATOR

Responsible to: Information Asset Owner

JOB SUMMARY
The Information Asset Administrator’s (IAA) primary role is to support the IAO to fulfil their responsibilities. IAA will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.

There are many categories of IA including:

- Information. Databases, system documents and procedures, archive media/data, paper records etc.
- Software. Application programs, system, development tools and utilities.
- Physical. Infrastructure, equipment, furniture and accommodation used for data processing.
- Services. Computing and communications, heating, lighting, power, air-conditioning used for data processing.
- People. Their qualifications, skills and experience in use of information systems.
- Intangibles. For example, public confidence in the organisation’s ability to ensure the Confidentiality, Integrity and Availability of personal data.

KEY RESPONSIBILITIES
Detailed responsibilities will be in agreement with the IAO – but would include:

1. Maintenance of Information Asset Registers
2. Ensuring compliance with Data Protection Act – data sharing agreements within the local area
3. Ensuring information handling procedures are fit for purpose and are properly applied
4. Under the direction of their IAO, ensuring that personal information is not unlawfully exploited
5. Recognising new information handling requirements (e.g. a new type of information arises) and that the IAO is consulted over appropriate procedures – e.g. completing/updating information mapping flows
6. Recognising potential or actual security incidents and consulting with the IAO
7. Reporting to the IAO on current state of local information handling
8. Ensuring that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the IAO
9. Act as first port of call for local managers/staff seeking advice on the handling of information
10. Under the direction of IAO, ensuring that information is securely destroyed at the end of the designation retention period
Appendix 3 – Terms of Reference of IG committees/ Groups

The revised Terms of Reference had not been approved at the presentation of this strategic plan refresh

<table>
<thead>
<tr>
<th>Title: Terms of Reference Clinical Management Board</th>
<th>East Cheshire NHS Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors Name: Chief Executive</td>
<td>Classification: Trust Organisation Structure and Minutes</td>
</tr>
<tr>
<td>Scope: Trust Wide</td>
<td>Replaces: Terms of Reference for Clinical Management Board February 2016</td>
</tr>
<tr>
<td>To be read in conjunction with the following documents: None</td>
<td></td>
</tr>
</tbody>
</table>

Unique Identifier: Review Date: February 2017 (or earlier if required)

Issue Status: V1 Issue No: 1 Issue Date: October 2016

Authorised by: Clinical Management Board Authorisation Date: October 2016

Document for Public Display: Yes

After this document is withdrawn from use it must be kept in an archive for 6 years.

Officer responsible for archive: Director of Corporate Affairs and Governance

1. Definition

- The Clinical Management Board has been established to manage the business of East Cheshire NHS Trust. It is the overarching forum for managing risks.

2. Purpose

- The Clinical Management Board will set the expected standard and provide assurance that management plans are in place to deliver the Board objectives and will ensure clinical engagement exists at the highest level of operational decision making by:
  - Developing the Clinical Strategy
  - Monitoring performance against key objectives
  - Ensuring strategic and corporate risks are being actively managed
• To shape annual and strategic plans
• Resolve operational issues, which have been escalated that impact across the Trust
• To ensure there is clear linkage with Service Lines and other Corporate Functions to deliver the business of the Trust

• This will facilitate a Leadership Team:
  ➢ Working as a team to manage the whole Trust by ensuring resources are targeted where they are most needed
  ➢ Being up to date with all the issues of the Trust and being familiar with benchmarking and good practice
  ➢ That challenges itself in striving to be the best
  ➢ That is recognised by other senior clinical and managerial colleagues for good communication and clarity of purpose

3. **Annual Work Programme**

**Work programme will be developed focusing on the highest risks.**

This will include:
• Systematic monitoring of all performance (Quality, Safety, Finance and Corporate Functions)
• Reviewing risks and management thereof
• Issues requiring CMB/Board approval
• Assurance to the Board on key issues via the Chief Executive
• An annual self-assessment of the achievements of the Clinical Management Board.

4. **Powers**

• To make operational decisions in line with the Scheme of Delegation.

5. **Frequency of Meetings**

• Monthly
• Members will be expected to attend for 75% of meetings and attendance registers will be maintained

6. **Membership**

• Executive Directors
• Clinical Directors of Service Lines
• Clinical Leads (from November 2016)

Other members may be co-opted to attend depending on the Agenda item.

7. **Reporting Groups**

The following groups will report to Clinical Management Board: key issues reported are slippage of agreed trajectories or changes/proposed developments, which impact on the business of the Trust, which will be mitigated through the corporate risk register:

➢ Capital & Space Planning
➢ Digital Transformation Group
➢ Pathology Executive Board
➢ Information Governance & Record Management Group (includes assurance requirements)
8. **Executive Management Team meeting**

This is the forum where Executive Directors are held to account by the CEO for delivery of objectives, recovery, which includes the delivery of the QIPP schemes. The Executive Management Team meeting is held weekly and supports timely decision making on business cases subsequently noted at the CMB.

9. **Quorum**

- 2 Executive Directors
- 3 Clinical Directors/or agreed representative

10. **Chairmanship**

   The Chair of the CMB will be the CEO or Deputy CEO (or another Executive Director in their absence)

11. **Conduct of Meetings**

   - Agendas will normally be prepared and circulated 5 days in advance of a committee meeting.
   - An Action Log of open and closed actions will be produced
   - Any member may request an item for the agenda through the chair
   - Any interest in the matter under discussion (as defined in Standing Orders) will be declared. The Person declaring an interest will withdraw whilst the issue is being discussed.
   - In the event of a formal vote, a simple minority will prevail. In the event of a tied vote the chair will have the deciding vote, provided that nothing is in the way business is conducted is prohibited in Standing Orders of the Trust

12. **Terms of Reference**

   These will be reviewed annually
1.0 Definition

1.1 The Trust Information Governance and Records Management Group has been established as a sub committee of the Clinical Management Board.

1.2 To provide a framework to ensure that all clinical and non-clinical information is managed legally, securely, efficiently and effectively. To provide reports to Clinical Management Board and highlight progress with IG Toolkit compliance and escalate any areas of concern.

1.3 To be responsible for ensuring that the Trust’s Policies, Procedures and Processes comply with legal requirements, best practice and Trust standards.

1.4 To ensure full compliance with both legal and best practice requirements: Connecting for Health ( CfH) Information Governance Toolkit, NHS Litigation Authority Risk Management Standards, Care Quality Commission Standards and the Royal College of Physicians.

2.0 Delegated Powers/Authority
2.1 Within its overall purpose and responsibilities and the requirements of the Corporate Governance Manual (Standing Orders, Standing Financial Instructions and the Scheme of Delegation) for the Trust the Group will have delegated power and authority within its overall purposes to:

- Ensure action is taken to achieve compliance in point 1.2 and 1.3 as outlined in definition.
- Investigate issues directly or indirectly
- Initiate action within the authority of its individual members or as delegated by the Clinical Management Board; propose further action to the Clinical Management Board.
- Develop and recommend strategies, policies, procedures and processes

2.2 The Group will operate within the overall strategies, policies and procedures agreed by the Trust Board or any of its Committees, although the Group may recommend changes to established strategies, policies and procedures as appropriate.

2.3 The Group may establish standing and/or time limited sub-groups as it sees fit for the effective conduct of its business. Terms of reference of any such sub-groups will be approved by the Information Governance and Records Management Group, except that all sub-groups will be subject to the limits of authority of the main group.

3.0 Responsibilities

3.1 To be responsible for Trust-wide co-ordination and prioritisation of all record management issues, including all clinical, non-clinical and corporate records information in accordance with the requirements contained within the IG Toolkit

3.2 To make recommendations to the Clinical Management Board for the development and improvement of services in relation to Information Governance and records management.

3.3 To monitor progress against key indicators identified in the CQC Regulations and other statutory and mandatory requirements, including the Information Governance Toolkit and ensure milestones are met. Ensure issues and risks are identified and escalated in a timely manner.

3.4 To highlight any related policies and procedures and submit to the responsible Director for ratification.

3.5 To maintain and scrutinise regularly a register of risks, escalating risks as required to Clinical Management Board.

3.6 To ensure appropriate governance arrangements for all written and electronic health care records including effective systems for the development and review of practice.

3.7 To provide assurance that the Trust is fully compliant with relevant legislation, namely the Data Protection Act 1998, Freedom of Information Act 2000 and specified Codes of Practice.

3.8 To monitor and report on the service delivered by Midland and Lancashire Commissioning Support Unit in relation to Information Security and Registration Authority and agree policies and procedures on behalf of Clinical Management Board.

3.9 To ensure that training in relation to information governance and records management is made available by the Trust, are fit for purpose and taken up by staff as necessary to support their role.
3.10 To receive external and internal audit reports and action plans to review and assess the implications for local policy and practice. Where required make additional recommendations as appropriate to the Directorates and Corporate Functions.

3.11 To monitor progress against the planned biennial corporate records management audit to ensure compliance against local policy and practice as well as legislated standards of record keeping.

3.12 To review and agree Information Sharing Agreements with external agencies and partners.

3.13 To review and monitor the Information Sharing Agreement log and Privacy Impact log (where appropriate), according to the schedule contained on the Information Governance & Records Management Group annual work plan.

3.14 To review and monitor, in accordance with the requirements outlined within the IG Toolkit, the Trust’s Data Mapping information.

3.15 To review and monitor, annually, the governance arrangements in relation to the transfer of Information overseas (in accordance with Data Protection Act – Principle 8).

3.16 To provide a focal point for the resolution and / or discussion of information governance issues.

3.17 To offer support, advice & guidance to the Caldicott function and data protection programme within the organisation.

4.0 Membership

4.1 Members of the Group will be:

- Director of Corporate Affairs and Governance (SIRO) (Chair)
- Caldicott Guardian (Associate Medical Director – Clinical Effectiveness)
- Deputy Caldicott Guardian
- Deputy Director of Corporate Affairs and Governance (Deputy SIRO)
- Head of Integrated Governance
- Integrated Governance Manager
- Information Governance Officer
- Media & Communications Manager
- Data Quality Representative
- Head of Informatics or other representative
- Business Partner, HR
- Information Security Manager (Midlands and Lancashire Commissioning Support Unit) or Representative
- Operational Manager - Outpatients
- Legal Services Manager
- Chief Clinical Information Officer, Consultant in Emergency Medicine
- Minimum of 2 x representative from each clinical directorate

Other officers will be co-opted as and when required.

4.2 Membership will be reviewed and confirmed by the Group on an annual basis and reported to the Clinical Management Board. Formal nominations for additional group members will be sought from Directors or Clinical Directors.

4.3 It is essential that where a group member is unable to attend that a deputy attends on their behalf.
4.4 In order to fulfil its responsibilities, the Group may invite others to attend particular meetings as observers or to speak about a specific item under discussion.

5.0 Quorum/Attendance

5.1 The quorum will be the Chair or deputy chair with at least 4 other members of the group and deputies will count towards the quorum.

5.2 Members, or their nominated representatives, are required to attend for 75% of meetings.

5.3 Where a member, or their representative, is unable to attend then apologies are expected prior to the meeting.

6.0 Chair

6.1 The Group will be chaired by the Senior Information Risk Owner

6.2 The deputy chair of the group will be the Caldicott Guardian (Associate Medical Director – Clinical Effectiveness/Consultant Rheumatologist)

7.0 Frequency and Calling of Meetings

7.1 The Group will meet bi-monthly, unless specific issues require the committee to meet prior to the set meeting date. Business may also be managed through virtual meetings with audit trails of decision making recorded.

8.0 Conduct of Business

8.1 Agendas will be prepared 2 weeks in advance, with circulation of the agenda and papers 1 week in advance of the meeting.

8.2 All papers will clearly state the agenda reference, the author, purpose of the paper and the action/decision to be taken.

8.3 Any member may place an item on the agenda and may propose any other business at a meeting which must be agreed with the chair at the start of or prior to the meeting.

8.4 Any interest in the matter under discussion (as defined in Standing Orders) will be declared. The person declaring an interest will withdraw whilst the issue is being discussed.

9.0 Minutes

9.1 All meetings will be minuted.

Minutes will be:

- Approved by the Chair before wider circulation
- Approved by the Committee at the next meeting of the Committee

9.2 Wider circulation should not be delayed until after approval by the group but should be clearly marked as DRAFT.
10.0 Reporting

10.1 The Data Quality Group shall report into this committee to provide assurance, through the provision of minutes of meetings and an annual assurance report. The group will also escalate any risks and issues as and when required.

10.2 The Health Records Management Sub-Group shall report into this committee to provide assurance, through the provision of minutes of meetings and an annual assurance report. The group will also escalate any risks and issues as and when required.

11.0 Public Access

11.1 Minutes and papers will be made available to members of the public on request subject to the provisions within the Freedom of Information Act 2000. Should an exemption be applicable, suitably edited minutes or papers will be made available.

12.0 Approval, review and variation of Terms of Reference

12.1 Any variation, including to the membership, will be informed to the Clinical Management Board.

12.2 The Clinical Management Board may formally request a change to the Terms of Reference at any time, either at its own initiation or following a request for variation submitted by the Group.

12.3 The Group will review the Terms of Reference annually and will be submitted to the Clinical Management Board if there are any changes.

12.4 The Group will review the Terms of Reference submitted in the light of the wider requirements of the Trust and may amend them before approval.

13.0 Performance

13.1 The group shall review its own performance, effectiveness and terms of reference on an annual basis.

13.2 The Group will submit an annual IG Toolkit report to Clinical Management Board for consideration, prior to formal publication of the assessment.
### Title: Caldicott Group

### Authors Name: Fiona Smith, Head of Integrated Governance

### Scope: All confidentiality/data protection issues

### Classification: Trust Organisation Structure and Minutes

### Replaces: v.2

### To be read in conjunction with the following documents:

<table>
<thead>
<tr>
<th>Unique Identifier:</th>
<th>Review Date: October 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This document is no longer authorised for use after this date</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issue Status:</th>
<th>Issue No: v.3</th>
<th>Issue Date: October 2017</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Authorised by: Senior Information Risk Owner</th>
<th>Authorisation Date: October 2017</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Document for Public Display: Yes</th>
</tr>
</thead>
</table>

After this document is withdrawn from use it must be kept in an archive for 6 years.

<table>
<thead>
<tr>
<th>Archive: October 2023</th>
<th>Date added to Archive:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Officer responsible for archive: Chair of the group</th>
</tr>
</thead>
</table>

### 13.0 Definition

13.1 The Caldicott Group has been established as a sub group of the Information Governance & Records Management Group.

13.2 To identify outstanding Caldicott issues.

13.3 To provide assurance that all actions necessary, in relation to Caldicott issues, have been taken and in accordance with the Caldicott Report (1997) and the guidance and recommendations contained within.
14.0 Responsibilities

14.1 To be responsible for Trust-wide review of all matters relating to patient confidentiality.
14.2 To be responsible for Trust-wide review of all incidents relating to disclosures made outside of the Data Protection Act (1998).
14.3 To provide assurance to the Information Governance & Records Management Group that all Caldicott incidents have been investigated and that all appropriate actions have been taken.
14.4 To provide assurance that the Trust is fully compliant with relevant legislation, when in receipt of requests for information, namely the Data Protection Act 1998, Freedom of Information Act 2000 and specified Codes of Practice.
14.5 To review all information sharing agreements relating to patient information to confirm that they comply with the requirements of the Data Protection Act. Identify and address any barriers for sharing for care.
14.6 To ensure members are kept up to date on the latest guidance on Caldicott, data protection and confidentiality principles through training and development

15.0 Membership

15.1 Members of the Group will be:

- Caldicott Guardian
- 1 x Deputy Caldicott Guardian
- Head of Integrated Governance (Chair)
- Integrated Governance Manager
- Information Governance Officer

Other officers will be co-opted as and when required.

15.2 Membership will be reviewed and confirmed by the Group on an annual basis.

15.3 The Group may invite others to attend particular meetings as observers or to speak about a specific item under discussion.

16.0 Quorum/ Attendance

16.1 The quorum will be the Chair with at least 1 other members of the group which must include the Caldicott Guardian or Deputy Caldicott Guardian.

16.2 Members, or their nominated representatives, are required to attend for 75% of meetings.

17.0 Chair

17.1 The Group will be chaired by the Head of Integrated Governance or, in their absence, the Integrated Governance Manager.
18.0 Frequency and Calling of Meetings

18.1 The Group will meet at least bi-monthly and a summary report will be provided twice yearly to the Information Governance & Records Management Group for formal review.

19.0 Conduct of Business

19.1 There will be no formal agenda as each meeting will concern itself with a review of the Caldicott Log:
- Information breaches reported on Datix
- Privacy Impact Assessments
- Information Sharing Agreements
- Caldicott related requests

20.0 Notes

20.1 All meetings will be noted and circulated to the Group for virtual approval.

21.0 Reporting

21.1 Summary report to be submitted twice yearly to the Information Governance & Records Management Group by the Caldicott Guardian (or their deputy).

Approval, review and variation of Terms of Reference

21.2 Any variation, including to the membership, will be informed to the Information Governance & Records Management Group

21.3 The Information Governance & Records Management Group may formally request a change to the Terms of Reference at any time, either at its own initiative or following a request for variation submitted by the Group.

21.4 The Group will review the Terms of Reference annually and these will be submitted to the Information Governance & Records Management Group if there are any changes

21.5 The Group will review the Terms of Reference submitted in the light of the wider requirements of the Trust and may amend them before approval.
<table>
<thead>
<tr>
<th>Title:</th>
<th>Data Quality Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors Name:</td>
<td>Mark Williams, Principal Information Analyst</td>
</tr>
<tr>
<td>Scope:</td>
<td>All information, collated, processed and maintained by East Cheshire NHS Trust</td>
</tr>
<tr>
<td>Classification:</td>
<td>Trust Organisation Structure and Minutes</td>
</tr>
<tr>
<td>Replaces:</td>
<td>N/A</td>
</tr>
<tr>
<td>To be read in conjunction with the following documents:</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier:</td>
<td>Review Date: November 2018</td>
</tr>
<tr>
<td>This document is no longer authorised for use after this date</td>
<td></td>
</tr>
<tr>
<td>Issue Status:</td>
<td>Draft</td>
</tr>
<tr>
<td>Issue No:</td>
<td>v.5</td>
</tr>
<tr>
<td>Issue Date :</td>
<td>30/11/2016</td>
</tr>
<tr>
<td>Authorised by:</td>
<td>Information Governance &amp; Records Management Group</td>
</tr>
<tr>
<td>Authorisation Date:</td>
<td>25/11/2016</td>
</tr>
<tr>
<td>Document for Public Display: Yes</td>
<td></td>
</tr>
<tr>
<td>After this document is withdrawn from use it must be kept in an archive for 6 years.</td>
<td></td>
</tr>
<tr>
<td>Archive:</td>
<td>Date added to Archive:</td>
</tr>
<tr>
<td>Officer responsible for archive: Chair of the group</td>
<td></td>
</tr>
</tbody>
</table>
1.0 Definition

1.1 The Data Quality Group has been established as a Sub-Committee of the Information Governance & Records Management Group (IGRMG).

1.2 It will provide a framework for integrated, patient based data quality throughout the organisation. To ensure the Trust is able to give assurance that information used for management reports, clinical audit and commissioning can be monitored and adjusted and that the quality of information meets the required standards of Information Governance to support the delivery of patient care. To provide regular reports to the IGRMG, highlighting any areas of concern.

1.3 To ensure compliance with the requirements contained in the Information Governance toolkit and the Healthcare Commission Healthcare Standards.

2.0 Delegated Powers/Authority

2.1 Within its overall purpose and responsibilities and the requirements of Standing Orders, Standing Financial Instructions and the Scheme of Delegation for the Trust the Group will have delegated power and authority within its overall purposes to

- Investigate issues directly or indirectly
- Initiate action within the authority of its individual members or as delegated by the IGRMG; propose further action to the IGRMG.
- Develop and recommend strategies, policies, procedures and processes
- Develop and agree organisational arrangements or refine arrangements within overall agreed structures and arrangements
- Establish working/steering groups, standing or ad hoc, and to agree their membership and other terms of reference

2.2 The Group will operate within the overall strategies, policies and procedures agreed by the Trust Board or any of its Committees, although the Group may recommend changes to established strategies, policies and procedures as appropriate.

2.3 Establishment of Groups reporting to the Data Quality Group:
   The Group may establish standing and/or time limited sub-groups as it sees fit for the effective conduct of its business.

3.0 Responsibilities

3.1 The Group will be responsible for Trust-wide co-ordination and prioritisation of data quality issues in relation to patient activity data

3.2 To provide strategic direction for the Trust in developing information quality assurance

3.3 The Group will propose modifications and enhancements to patients systems, most notably the Patient Administration System (PAS)

3.4 To co-ordinate external data quality audits and to produce proposals in the light of results

3.5 To implement and monitor internal data quality audits and to produce actions plans to manage results

3.6 To filter proposals emanating from user groups for PAS and other systems including where these impact on paper-based processes
3.7 To make recommendations to the IGRMG for the development and improvement of services in relation to information quality

3.8 The Group will monitor progress against key indicators identified for information quality in the Information Governance Toolkit and the healthcare standards

3.9 To include other principal systems where these impact upon integrated data and the MPI

3.10 To approve any data quality related policies and procedures and submit to the IG&RM Group for ratification

3.11 The Group will maintain and scrutinise regularly a register of risks, reporting as required to the IGRMG.

3.12 The Group will monitor data quality benchmarking reports (as delivered by SUS) and be responsible for actioning any proposals to rectify emerging issues.

4.0 Membership

Members of the Group will be:-

- Principal Information Analyst (Chair)
- Community Systems Manager
- Booking, Capacity & Reception Manager
- PAS Manager
- Clinical Coding Manager
- Information Governance Officer
- Finance Systems Manager
- Urgent Care Administration Manager
- Interface Support Representative
- Radiology Systems Manager
- (Further members to be co-opted as appropriate)

The following will be in attendance as advisors to the Group as and when required:

- Maternity System Manager
- Theatre System Manager

Membership will be reviewed and confirmed by the group on an annual basis and approved by the IGRMG. Formal nominations for additional group members will be sought from Executive Directors or Clinical Heads of Service.

Where applicable, deputys will attend for principals who are unable to attend. However, deputys for members will be in attendance rather than taking the full rights and responsibilities of the member, except where the deputy is formally acting up for the member as defined in Trust Standing Orders.

Members or their representatives are required to attend for 75% of meetings.

The Group may invite others to attend particular meetings as observers or to speak about a specific item under discussion.

5.0 Quorum

The quorum will be at least 4 members of the Group. Deputies will not count towards the quorum except when covered by formal acting up arrangements as defined in Trust Standard Orders. Those in attendance will not count towards the quorum.
6.0 Chair
The Group will be chaired by the Principal Information Analyst.

7.0 Frequency and Calling of Meetings
The Group will meet every other month, unless specific issues require the Group to meet in the interim period.

8.0 Conduct of Business
An agenda will be prepared and circulated in advance of the meeting.

Any member may place an item on the agenda and may propose any other urgent business at a meeting. Other business may be placed on the agenda at the request of an attendee and with the agreement of the Chair.

Members will have the right to speak and if necessary vote at meetings of the Group. Attendees may speak and their opinions may be sought but they will not participate in any formal vote.

Any interest in the matter under discussion (as defined in Standing Orders) will be declared. The person declaring an interest will withdraw whilst the issue is being discussed.

In the event of a formal vote, a simple majority will prevail. In the event of a tied vote the Chair will have a deciding vote.

9.0 Minutes
All meetings will be minuted.

Minutes will be:
- Approved by the Chair before submission to the IGRMG or wider circulation
- Approved by the Group at the next meeting of the Group

Submission to the IGRMG or wider circulation should not be delayed until after approval by the Group but should be clearly marked as not yet fully approved.

10.0 Reporting
Minutes of the Group will be presented to the IGRMG by the Chair or nominated representative.

Annual assurance report will be provided to the IGRMG.

11.0 Public Access
Minutes and papers will be made available to members of the public on request subject to the provisions within the Freedom of Information Act 2000. Should an exemption be applicable, suitably edited minutes or papers will be made available.
12.0 Approval, review and variation of Terms of Reference

These Terms of Reference were approved by the Data Quality Group at its meeting on 22nd November 2016 and ratified by the Information Governance Group following circulation for virtual agreement as agreed at its meeting on Tuesday 25th November 2016.

The Group will review the Terms of Reference annually for approval at the IGRMG. The Information Governance and Records Management Group will review the Terms of Reference submitted in the light of the wider requirements of the Trust and may amend them before approval.
Title: Health Records Management Sub-Group

Authors Name: Pam Laird, Integrated Governance Manager

Scope: All records used and maintained by East Cheshire NHS Trust

Classification: Trust Organisation Structure and Minutes

Replaces: Version 2

To be read in conjunction with the following documents:
Information Governance & Records Management Group

Unique Identifier: HRMSG-TOR/V.3

Review Date: June 2018

This document is no longer authorised for use after this date

Issue Status: Draft

Issue No: 3

Issue Date: June 2016

Authorised by: Information Governance & Records Management Group

Authorisation Date: 16.06.16

Document for Public Display: Yes

After this document is withdrawn from use it must be kept in an archive for 2 years.

Officer responsible for archive: Integrated Governance Manager

1.0 Definition

1.1 The Health Records Management Sub-Group has been established as a Sub-Group of the Information Governance & Records Management Group to ensure that all the organisation’s health records are managed legally, securely, efficiently and effectively.

2.0 Delegated Powers/Authority

2.1 The Sub-Group will be subject to the limits of authority of the main group.

3.0 Responsibilities

3.1 To assist IGRMG in Trust-wide co-ordination and prioritisation of all health record management issues.

3.2 To make recommendations to the IGRMG for improvements in relation to policy and/or practice relating to records management.
3.3 To review operational issues relating to health records management as delegated by IGRMG including assistance to IGRMG in its function to ensure full compliance with both legal and best practice requirements: Connecting for Health (CfH) Information Governance Toolkit, NHS Litigation Authority Risk Management Standards, Care Quality Commission Standards, Dept. of Health Records Management Code of Practice.

4.0 Membership

4.1 Members of the Group will be:-

- Caldicott Guardian (Chair)
- Chief Clinical Information Officer
- Integrated Governance Manager
- Information Governance Officer
- Outpatient Services Manager
- Outpatient Department Administration Manager
- Health Records Library Team Leader
- Ward Administration Support
- Clinical Administration Manager
- Representation from each Service Line
- Representation from Legal Services

Other officers will be co-opted as and when required.

4.2 Membership will be reviewed and confirmed by the Sub-Group after an initial 6 month period from the date of ratification, thereafter on a biennial basis and reported to the Information Governance & Records Management Group.

4.3 The Group may invite others to attend particular meetings as observers or to speak about a specific item under discussion.

5.0 Quorum/ Attendance

5.1 The quorum will be the Chair with at least 4 other members of the group and deputies will count towards the quorum.

5.2 Members, or their nominated representatives, are required to attend for 75% of meetings.

6.0 Chair

6.1 The Group will be chaired by the Caldicott Guardian

6.2 The IG Officer to be responsible for drafting and circulating the Health Records Management Sub-Group agenda as well as arranging admin. provision for recording the notes.

7.0 Frequency and Calling of Meetings

7.1 The Group will meet bi-monthly, on the 4th Tuesday of the month, on alternate months to the IGRMG set meeting dates, unless specific issues require the committee to meet prior to the set meeting date. Business may also be managed through virtual meetings with audit trails of decision making recorded.
8.0 Conduct of Business

8.1 Agendas will be prepared and circulated one week in advance.

8.2 Any member may place an item on the agenda and may propose any other business at a meeting which must be agreed with the chair at the start of or prior to the meeting.

8.3 Any member not able to be present or to arrange a representative, must provide feedback on any open Action Log items.

9.0 Notes

9.1 Notes will be produced for each meeting.

    Notes will be:
    
    - Approved by the Chair before submission to the IGRMG
    - Formally approved by the sub-Group at the next meeting of the sub-Group

10.0 Reporting

10.1 To be directly responsible to the IGRMG and to feedback to the IGRMG on a regular basis, via the notes of meetings.

10.2 Notes of the meetings will be presented to the IGRMG by the Chair of the Sub-Group, or a Group member in the Chair’s absence.

11.0 Public Access

11.1 Notes and papers will be made available to members of the public on request subject to the provisions within the Freedom of Information Act 2000. Should an exemption be applicable, suitably edited minutes or papers will be made available.

12.0 Approval, review and variation of Terms of Reference

12.1 Any variation, including to the membership, will be informed to the Information Governance & Records Management Group

12.2 The Information Governance & Records Management Group may formally request a change to the Terms of Reference at any time, either at its own initiation or following a request for variation submitted by the Group.

12.3 The Group will review the Terms of Reference biennially and will be submitted to the Information Governance & Records Management Group if there are any changes

12.4 The Group will review the Terms of Reference submitted in the light of the wider requirements of the Trust and may amend them before approval.
APPENDIX 4 – Strategy for Clinical Involvement in Activity Recording and Coding

The Information Strategy and the Data Quality Policy allude to the need for increasing clinician involvement in data collection, coding and validation. The results of several audits also include the need to more fully engage with clinicians in data collection – especially within the clinical coding area. There are several key areas where it would be profitable to involve clinicians in data collection and validation:

- Clinical Coding – access to clinicians
- CQC / Dr Foster alerts
- Mortality Review Sub-committee
- Clinical Audit
- Community Clinicians
- Clinician Self-coding

**Clinical Coding – Access to Clinicians**
The senior clinical coder should be routinely invited to service line clinical meetings to discuss coding related issues and developments e.g. clinical audit meetings. Clinical coders should be given access to clinicians to resolve any day to day coding problems and may include such things as accompanying clinicians on ward rounds.

Clinicians working within community settings will be engaged with as the trust continues to build on the data validation discussions. This is particularly important as the new EMIS Web system is rolled out to the full range of community services.

**Care Quality Commission (CQC) / Dr Foster Alerts**
Clinicians will inevitably be involved with deep data validation when any CQC / Dr Foster alert is received by the Trust. It is recommended that clinical coders, amongst other Informatics staff, are equally involved in any alert investigations. It is further recommended that clinicians routinely monitor the clinical results contained within the Trust’s CHKS system and contact the Information Team or the Clinical Coders where any queries are raised.

**Mortality Review Sub-committee**
The Mortality Review Sub-committee will receive regular reports from the Information Team. These will consist of “crude” deaths in hospital split by ward, “crude” deaths in hospital by day of week, and a list of “unexpected” deaths drawn from the CHKS system. The results of these, especially the “unexpected” deaths, will be forwarded to the relevant service line where it is expected that clinicians will investigate and validate the results.

This sub-committee provides assurance via the Trust Safety and Quality and Standards Committee.
Clinical Audit
The Trust will continue with its Clinical Audit programme, which includes validating the data collected on Trust systems. Outcomes of the annual Clinical Coding Audit will be shared with clinical audit Leads.

Clinician Self-Coding
The possibility of clinicians coding directly into Trust systems will continue to be examined. This will include coding directly into the Theatre system, the electronic Discharge Notification System (eDNF) and the Extramed ED system. Consideration should also be given to the purchase of an electronic, integrated encoder which would allow clinicians to code patient episodes on the Patient Administration System (PAS). Professional coders would then be required to review the clinician coding.

APPENDIX 5 - Acronyms

CQC – Care Quality Commission
DH – Department of Health
IG – Information Governance
IGT – Information Governance Toolkit
SIRO – Senior Information Risk Owner
SUS – Secondary Users Service Data
ToR – Terms of Reference
IGRMG – Information Governance & Records Management Group
ED – Emergency Department