

Data Quality Policy

Document Reference No.	KMPT.InfG.007.06
Replacing document	KMPT.InfG.007.05
Target audience	Trust wide
Author	Director of Contracting, Performance & information
Group responsible for developing document	Information Governance Group
Status	Authorised
Authorised/Ratified By	Information Governance Group
Authorised/Ratified On	April 2021
Date of Implementation	April 2021
Review Date	April 2024
Review	This document will be reviewed prior to review date if a legislative change or other event otherwise dictates.
Distribution date	April 2021
Number of Pages	12
Contact Point for Queries	kmpt.policies@nhs.net
Copyright	Kent and Medway NHS and Social Care Partnership Trust 2021

DOCUMENT TRACKING SHEET

Data Quality Policy

Version	Status	Date	Issued to/approved by	Comments
1.0	Approved	25.09.07	Information Governance Group	Approved for Use
2.0	Approved	March 2010	Information Governance Group	Approved for Use
3.0	Approved	October 2012	Information Governance Group	Approved for Use
4.0	Approved	February 2015	Information Governance Group	Approved for Use
4.1	To be approved	February 2017	Information Governance Group	Refreshed to reflect MHSD, DQ responsibilities of PMMs and current Management responsibilities
5.0	Approved	Feb 2017	Information Governance Group	Approved for use
5.1	Approved	August 2017	Policy Manager	Separated Equality Impact Assessment from document.
5.2	DRAFT	July 2020	Data Quality Group	For comment / update / approval
5.3	DRAFT	August 2020	Phil Lawrence – Director of Contracting Performance & Information	Updated following comments received from the DQ Group
5.4	FINAL	March 2021	Data Quality Group	Approved for ratification at Information Governance Group
6.0	FINAL	6 April 2021	Information Governance Group	Ratified

RELATED POLICIES/PROCEDURES/protocols/forms/leaflets

Information Security Policy	KMPT.InfG.002
Overarching Information Sharing Policy	KMPT.InfG.065
Health and Social Care Records Policy	KMPT.InfG.071

SUMMARY OF CHANGES

Date	Author	Page	Changes (brief summary)

CONTENTS

1	INTRODUCTION	1
2	PURPOSE	1
3	INFORMATION SYSTEMS	2
4	ROLES AND RESPONSIBILITY	3
5	DUTIES	3
6	DATA QUALITY REQUIREMENTS	6
7	MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THIS DOCUMENT	8
8	IMPLEMENTATION INCLUDING TRAINING AND AWARENESS	8
9	SYSTEM SPECIFIC DATA QUALITY PROCEDURES.....	8
10	SECURITY	11
11	KEY PERFORMANCE INDICATORS	11
12	EQUALITY IMPACT ASSESSMENT	11
13	HUMAN RIGHTS.....	12
14	CONCLUSION.....	12

1 INTRODUCTION

- 1.1 Kent and Medway NHS and Social Care Partnership Trust (KMPT) recognises the importance of reliable information to support the quality of care and provision of effective and safe treatment of its service users. In addition, in order to succeed as a health and social care organisation in the current market it is essential that KMPT can demonstrate and understand its performance in service delivery, governance, finance, workforce, and business development.
- 1.2 The Trust recognises that reliable information can only be produced if good quality data is captured at source, regardless of the methods used to capture this data. It is therefore the aspiration of the Trust that 100% data accuracy is achieved by its employees when collecting and transcribing data items. The Trust will support the development of individuals, processes and systems to minimise the risk of data errors.
- 1.3 Data quality is primarily a clinical function as they are responsible for the completeness and accuracy of records. Support services provide the tools, knowledge and guidance to support the data quality process. This is through system support teams, Business Intelligence team and Information Governance.
- 1.4 Poor data quality is one of the main threats to the Trust failing to achieve its strategic objectives and has a wide variety of implications on the efficient running of the Trusts services including:
 - Preventable serious incidents occurring
 - Poor management decisions being made (e.g. Resourcing/Planning)
 - Loss of income
 - Lack of confidence/credibility in the Trust from external bodies and patients/service users
- 1.5 Effective performance management requires accurate, relevant and timely information. Where there is poor quality data, the usefulness of performance information is reduced and the credibility of the performance process undermined. The Data Quality Strategy will support the delivery of the Trusts Performance Management Framework, it aims to foster a culture of responsibility and accountability for data quality involving everyone at all levels in the Trust.

2 PURPOSE

- 2.1 This policy aims to outline the process for ensuring that the quality of data is maintained to support patient care, clinical governance, finance, workforce, and business development.
- 2.2 The purpose of this policy is to ensure that the relationship between good quality data, good quality information, and good quality decisions is clearly understood and that the responsibilities for the management of that relationship are identified for everyone at all levels in the Trust.
- 2.3 Ever-increasing use of computerised systems provides greater opportunities to store and access many types and large volumes of data but also increases the risk of misinformation if the data from which information is derived is not of good quality. This risk applies both to the Trust's internal use of information and to information conveyed in the form of statutory returns to the national databases. For information to have value, it is essential that the data

that underlies it is consistent and complies with national standards.

- 2.4 It is intended to raise awareness of the increasing reliance of the organisation on good data quality and the responsibilities of staff to support the information requirements of the wider organisation as well as meet their local needs.

3 INFORMATION SYSTEMS

- 3.1 The Policy applies to all corporate information that is entered onto a computerised system whether centrally or locally maintained.
- 3.2 Whilst the main emphasis is on the Trust Patient Information System RiO and in the supporting Business Intelligence reports, all Trust computerised systems are included.
- 3.3 Summary details of the Trust's primary electronic information systems are set out below:

Table 1 – Trust Electronic Information Systems

System	Types of Service using the System	Scope of system
Rio	All Trust services with the exception of Psychological Therapies in Primary Care	Primary electronic health and social care record.
Business Intelligence (BI)	All Trust services using Rio and PLICs	Bespoke reporting system providing operational management and summary performance reports from Rio and PLICs
Insight	Trust Managers using RiO	Interactive dashboards to support management decisions
SBS	All services within the Trust	The SBS general Ledger is a fully integrated financial administration and management system incorporating Invoice processing (income and payments), purchase order processing and general ledger transaction processing (journals and budgets updates).
Patient Level Costing System (PLICs)	All services within the Trust	Analyses cost by Service Line to Patient Level, as well as detail of the activities associated with the care provided
Datix	Non Clinical Risk assessors and managers and Health and Safety Team, KMPT Legal team, Complaints and PALS management, RFI management, Safety Alert Co-ordinator	Risk Management system capturing and managing all Trust patient safety data within one system including risk, complaints and incident related themes and trends.
ESR	HR & Payroll	Electronic Staff Record (ESR) is a national HR/Payroll system that has been designed and developed to be the comprehensive, integrated workforce management system which will deliver the workforce strategy for the NHS.

MAPS Suite – e-Rostering and e-Expenses	Health and	All staff	eRostering is an electronic way of efficiently managing when staff are required for work. e-Expenses functionality is used to monitor and manage staff travel and other expense claims
---	------------	-----------	--

4 ROLES AND RESPONSIBILITY

- 4.1 The policy applies to systems, electronic or otherwise, which collect, store or report on data related to the activities of the Trust.
- 4.2 The Trust should ensure wherever possible that electronic systems feed performance reports internally and externally as these are more reliable. It is recognised that there may be exceptions when electronic systems are unable to report specified and agreed information, and in such cases manual data reports would need to be developed. The development of such manual information systems should be kept to an absolute minimum and agreed with the relevant Director. Where they do exist, it is the responsibility of the reporting officer to ensure that data quality processes are in place and that all information reported internally or externally has been validated in support of this Policy,
- 4.3 This policy will also apply to new systems implemented post publication of this policy.
- 4.4 The policy applies to:
 - 4.4.1 All staff employed by, or seconded to, KMPT who use Trust information systems
 - 4.4.2 All staff employed by, or seconded to, KMPT who collect information for entry onto Trust information systems.
- 4.5 Appropriate groups within the trusts performance management structures will be responsible for implementing the policy with issues and risks escalated as required.
- 4.6 This policy must be read alongside Trust Performance Strategy and Performance Management Framework, Health Records Management Policy, Standards for Record Keeping, Rio and other system guidance such as standard operating procedures for information systems, and professional codes of conduct.
- 4.7 This policy outlines good practice and identifies the roles and responsibilities of both the Trust and staff in terms of data quality.

5 DUTIES

SPECIFIC DATA QUALITY RESPONSIBILITIES

- 5.1 Ultimate responsibility for data quality lies with the Executive Director of Finance.
- 5.2 The Director of Contracts & Performance and the Assistant Director of Information and Performance will be responsible for the operational management of data quality.
- 5.3 The Caldicott Guardian is responsible for ensuring that patient information is handled and processed in accordance with Caldicott requirements.
- 5.4 The Data Protection Officer is responsible for ensuring that patient information is maintained to meet Data Protection requirements and supporting any responses to patients who make formal complaints about information that is held.

GENERIC DATA QUALITY RESPONSIBILITIES

- 5.5 A number of key groups and individuals have responsibilities in relation to data quality. These are as follows:
- 5.6 **Trust Board**
- 5.6.1 Prime responsibility for the quality of data rests with the organisation producing it.
 - 5.6.2 It is the responsibility of the Board to ensure policies and procedures are in place that ensures data and therefore information is of good or at least known quality.
 - 5.6.3 To establish assurance processes to monitor data quality and mechanisms to take action to improve it where necessary.
 - 5.6.4 To approve the data set requirements of the organisation and ensure mechanisms exist which facilitate the capture of good data quality.
- 5.7 **Executive Directors**
- 5.7.1 Responsible for accurate Data Quality within their corporate areas of responsibility including relevant Information Asset Owners (IAO).
 - 5.7.2 Responsible for ensuring their data set is collectable and appropriate resources and procedures are in place to collect it.
 - 5.7.3 Ensure that the quality of data issued from their areas is of good quality.
 - 5.7.4 Ensure that their service meets definitions for Data Quality where defined for core data sets and mandatory data collections
 - 5.7.5 Monitor performance against data quality standards ensuring corrective action is taken where necessary.
 - 5.7.6 Maintain compliance with changes by keeping up to date with current standards and consulting with relevant in house expertise where applicable i.e. Information Governance.
- 5.8 **Information Management and Central Performance Function:**
- 5.8.1 Maintain and develop a central data repository which will support the production and development of information and data quality reporting.
 - 5.8.2 Feedback any intelligence on data quality from the data entered on the systems where it is available and develops appropriate data quality monitoring tools.
 - 5.8.3 Interpret and advise requirements of the clinical Data Dictionary and Data Manual to ensure compliance.
 - 5.8.4 Monitor and disseminate changes to requirements as notified via NHS Digital or other official channels as appropriate.
 - 5.8.5 Manage validation programmes used routinely on data entry to ensure completeness and validity of national data sets submissions as appropriate.
 - 5.8.6 Advise clinical teams, managers and board on Information issues.
 - 5.8.7 Consult as required with clinical /other expertise on Information quality matters.
- 5.9 **Heads of Service**
- 5.9.1 Heads of Service are operationally responsible for the quality of data for their Care Group.

- 5.9.2 Overall responsibility to develop and implement local action plans for improvement.
- 5.9.3 To ensure adequate resource allocation, training, management and assurance are in place supported by consistent local procedures.
- 5.9.4 Ensure data sets and all mandatory data requirements can be collected and that the service adheres to defined data definitions and requirements where appropriate.
- 5.9.5 To implement local processes for quality assurance and utilise tools and systems provided by the organisation to maximum effect to improve quality.
- 5.9.6 Seek advice from internal expertise and comply with best practice and advice.

5.10 Managers:

- 5.10.1 Ensure all staff for which they are responsible input accurate and complete data in a timely manner, consistent with all relevant policies and information governance standards.
- 5.10.2 Supervise staff and ensure training is up to date and utilise data quality tools where supplied to improve the quality of data.
- 5.10.3 Ensure corrective actions and measures are implemented within deadlines for reporting submissions.
- 5.10.4 Ensure staff are aware of their responsibilities with regard to regularly checking and resolving inaccuracies and quality assure their work.
- 5.10.5 Set up local procedures and supporting guidelines. Where trust wide systems exist – the local procedures must be consistent across all areas.
- 5.10.6 Take local responsibility for the quality of data and feedback particular issues for training or update of procedures, including resolution of data subject's issues.
- 5.10.7 Ensure that all appropriate job descriptions contain reference to the responsibility of roles with respect to recording information and ensuring accuracy and completeness of data.
- 5.10.8 Ensure all staff are trained in and are familiar with and adhere to current legislation, policies and procedures.
- 5.10.9 Address data quality issues as soon as possible and escalate appropriately through agreed formal channels.

5.11 All Staff

- 5.11.1 Ensure timely, accurate and complete data is recorded and entered appropriately.
- 5.11.2 Identify errors and omissions as close to the point of entry as possible and correct at source.
- 5.11.3 Monitor and escalate any data quality issues identified appropriately to their line manager and /or agreed formal channels.
- 5.11.4 Data quality is every ones responsibility and staff must not rely on others to carry out their data quality responsibilities.
- 5.11.5 Monitor own competencies and access appropriate training where necessary.
- 5.11.6 Staff must be aware of and comply with legislation, Trust policies and procedures.
- 5.11.7 All staff who deal with any form of data and or/information are responsible for ensuring data quality is consistently maintained.

6 DATA QUALITY REQUIREMENTS

6.1 Within this policy the term “data” refers to numbers, words or images that have yet to be organised or analysed to answer a specific question

6.2 To maintain and demonstrate quality it is necessary to ensure that data are:

- Accurate
- Complete
- Timely
- Valid
- Consistent
- Available
- Compliant with NHS standards and legal requirements
- Audited

6.3 ACCURACY

6.3.1 Staff must ensure that information systems, or paper records for subsequent data entry, accurately reflect what actually happened.

6.3.2 Patient demographic details should be checked with the patient themselves each time they are seen and any changes made to the electronic record.

6.3.3 All reference tables, such as GP’s and postcodes, will be updated regularly.

6.3.4 System Administrators must be advised when changes occur which necessitate changes to system reference tables, e.g. staff changes, staff leavers, changes of base, introduction of new services, and reconfiguration of existing services.

6.4 COMPLETENESS

6.4.1 All mandatory data items within a data set must be completed.

6.4.2 Wherever possible, the system must force the capture of mandatory data items.

6.4.3 Use of default codes will only be used where appropriate, and not as a substitute for real data.

6.4.4 If is necessary to bypass a data item in order to register that patient, the missing data must be reported for immediate follow up.

6.5 TIMELINESS

6.5.1 Data must be entered into systems as soon as practicable after the event/decision.

6.5.2 To ensure the safe and effective care/treatment of service user data should be recorded in a timely fashion in accordance with policy and guidance. Up to date entry of interventions and contacts guarantees that all professionals have access to the latest known information pertaining to service users. This practice also ensures that up to date data can be included in national, local and internal reports.

6.5.3 Paper information (central data entry) will be submitted in line with current guidance and practices and must adhere to the Data Quality Policy.

6.6 VALIDITY

- 6.6.1 All data items held on trust computer systems must be valid.
- 6.6.2 Where codes are used, those will comply with national standards or will map to national values
- 6.6.3 Wherever possible, computer systems will be programmed to only accept valid entries.

6.7 CONSISTENCY

- 6.7.1 Data items must be internally consistent. Operational Service Lines Standard Operating procedures are to be adhered to in all cases.
- 6.7.2 Consistency checks will be undertaken against information systems and manual records.

6.8 AVAILABILITY

- 6.8.1 Staff must have access to information systems in accordance with their role and responsibility.
- 6.8.2 Access to information systems will be available 24 hours/day.
- 6.8.3 Summary and detailed information reports are available by request or by direct access as is the case of BI, Insight and PLICS.

6.9 MONITORING, AUDIT AND BENCHMARKING

- 6.9.1 Benchmarking of performance will be a key tool in assessing levels of data quality including:
 - MHSDS Reports for national comparison
 - Mental Health NHS Benchmarking club for national comparison
 - Trust Integrated Quality and Performance Report (IQPR) for trust wide benchmarking
 - BI and Insight for local team and individual benchmarking
- 6.9.2 The Trust will continue to audit its data quality within reports to ensure that the quality of the data
- 6.9.3 All data systems must have an audit trail and that must be turned on and used
- 6.9.4 Reports highlighting weakness in data quality will be issued to relevant staff in accordance with relevant systems
- 6.9.5 KMPT's Business Intelligence systems (BI & Insight) will be designed to highlight data quality errors within operational reports as well as producing reports summarising Data Quality issues.
- 6.9.6 Records Officers will undertake annual audits each year. The information will be compiled on a yearly basis, action plans resulting from the audit will be reviewed by the Information Governance Group..
- 6.9.7 Audits covering accuracy checks on service user data will be regularly carried out and will cover all key data items
- 6.9.8 Audits covering completeness and validity will be carried out in line with guidance from the IG Toolkit

- 6.9.9 System Administrators and support teams will undertake an annual programme of system audits these will ensure consistency of Information held in separate systems.
- 6.9.10 Data quality reports from external sources will be utilised to assess and monitor data quality. Areas of concern to be identified by AD of Information and Performance and reported to the appropriate QPR's
- 6.9.11 Internal audits will be conducted on a regular basis to provide independent assurance on Data Quality to the Trust Board.

7 MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THIS DOCUMENT

- 7.1 The Data Quality Group is responsible for the monitoring of this policy.
- 7.2 The Group will act as a sub group of the Information Governance Group and will produce regular reports on:
 - 7.2.1 Current levels of data quality
 - 7.2.2 Data quality issues
 - 7.2.3 Progress on data quality initiatives
- 7.3 This policy will be reviewed and/or revised on a yearly basis.
- 7.4 Where there is evidence of non-achievement of compliance, appropriate action will be taken to remedy the situation and to raise awareness of the policy implementation requirements.

8 IMPLEMENTATION INCLUDING TRAINING AND AWARENESS

- 8.1 Additional support can be provided by the departments who administer the relevant system such as the RiO Support team and the Information Management Team.
- 8.2 Ongoing training to support the awareness and action to improve data quality will include BI and Insight, RiO systems training and Information Governance.
- 8.3 All staff must receive any specified training before being given access to information systems.
- 8.4 Training will include requirements for maintaining data quality.
- 8.5 Staff will have access to procedure notes which include details of data quality responsibilities.

9 SYSTEM SPECIFIC DATA QUALITY PROCEDURES

- 9.1 **RiO**
 - 9.1.1 Annual audits are conducted with recommendations/action plans produced; these are monitored by the Health and Social Care Records User Group.
 - 9.1.2 In addition the Information Governance and Records Management Team complete ad hoc audits in response to issues raised.

9.2 ESR

- 9.2.1 ESR is a national system that produces monthly data quality reports sent to the trust via the ESR Central team which deals with most areas of data. In addition KMPT staff run data quality checks including reviews on teams as part of integration with MAPS and other HR Systems.

9.3 SBS

- 9.3.1 The system forms the core of the Trusts financial management and reporting.
- 9.3.2 The Trust relies on the service level agreement with SBS to ensure that the system has adequate and maintained internal controls to ensure accuracy of transactions and reports.
- 9.3.3 Every year, a programme of systematic and regulatory financial system audits are undertaken both by internal and external audit to give assurance that the system is functioning as intended from all aspects of data quality and security.
- 9.3.4 The Trust also performs secondary internal checks in the form of regular monthly control account reconciliations which have to be signed off each month by the head of financial control.
- 9.3.5 The monthly financial management reporting cycle also involves a data quality review through management accountants undertaking trend and variance analyses for their respective Service lines and cost centres. The periodic financial reports produced through this process are reconciled to the ledger and any material manual adjustments are noted / highlighted.
- 9.3.6 Data inaccuracies picked up in these monthly reporting cycles are corrected through journal transactions and review of data sources and processing where the inaccuracies are deemed systematic.
- 9.3.7 All manually generated input journals are required to be signed off by senior Finance managers to ensure that transactions are correctly undertaken and are accurate.
- 9.3.8 The departmental risk register picks up any risks to data accuracy that finance managers become alerted to. Where necessary, remedial action are implemented to manage the risk.

9.4 PLICS

- 9.4.1 PLICS is the Trusts patient level information costing system that regularly takes in actual cost information from the finance ledger (SBS) and processes these to derive treatment costs at patient level. PLICs output will be a central basis for contract income and billing as well as performance management within the Trust so system accuracy is fundamental to its functionality.
- 9.4.2 Control processes:
- 9.4.3 Financial data imported into PLICS each month is reconciled to the ledger as part of the monthly data migration process. The system has inbuilt control reports that will alert the system administrator of any imbalances or mismatch of data.
- 9.4.4 Clinical Activity data is directly imported from BI through an automated interface process. Data reconciliation controls similar to that described above are incorporated into the upload routine and any mismatches are resolved by the PLICS system administrator before the upload can be completed.

- 9.4.5 Ideally there should be a process by which new or changed attribute values such as New teams (or team references) can be flagged up to the PLICS system administrator at the point of update into Rio, to ensure that all relevant impacts of the update are effectively reviewed and acted upon within PLICS.
- 9.4.6 The accuracy of data mapping and cost allocation is dependent upon the allocation rules and apportionment tables maintained in the PLICS system. Regular / periodic updates of the apportionment tables are reviewed by the senior Finance PLICS lead prior to acceptance. All other accuracy checks are incorporated into the reasonableness checks that are undertaken each month by the management accountants as part of their monthly review and preparation of PLICS performance reports. Service Line managers are also required to feedback (to finance) any unusual or incorrect information produced by the system.
- 9.4.7 Recent reviews have indicated that historic monthly PLICS uploads progressively get out of sync with BI data because BI accepts backdated transactions so subsequent reconciliations between PLICS reports and BI reports will indicate variances. We are currently considering alternative work around to resolve this issue.

9.5 **Datix**

- 9.5.1 The rollout of the Datix risk management system now provides regular reporting at Board, service line and ward level of incident and complaints activity, along with non clinical risks. This reporting has allowed focus on patient safety incident related themes and trends leading to the implementation and monitoring of service improvement plans. Managing all Trust patient safety data within one system is increasing the visibility of the data across the Trust, leading to improved data quality.

9.6 **BI & Insight**

- 9.6.1 The development of BI and Insight, as the Trust's reporting system, will be focussed on providing a wide range of information on services, initially from Rio and PLICS, in a user-friendly manner, to the widest possible audience so that clinicians and managers can understand the quality and performance of their services.
- 9.6.2 The Business Intelligence (BI) system within KMPT at present is a reporting tool that reflects the extract of RiO received by the trust each night, it is therefore essential that processes are put in place to ensure the data presented in BI each day is validated.
- 9.6.3 Insight aims to capture information from numerous systems to support data triangulation which will give greater intelligence to inform practices that may improve data quality.
- 9.6.4 A number of processes exist within the information management team which validate each overnight deployment of the previous days update. Reports track each stage of the deployment and the first task for the IM team each day is to ensure all processes have completed successfully and investigate any exceptions. Further checks of the accuracy of the extract are carried out by comparing the table row counts against the previous day, in the event of a discrepancy the data would not be loaded onto the BI portal until deemed valid.
- 9.6.5 A traffic light system and announcements section is present on the homepage of the web based portal to advise users of any data quality issues.

10 SECURITY

- 10.1 All staff who work within the Trust and those staff who have been seconded to the Trust are bound by their common code of Confidentiality, the Data Protection Act 2018 and the non-ethical code of practice, not to divulge any personal information without authorisation.
- 10.2 Staff will not be given access to information systems unless they have received appropriate training.
- 10.3 Access to information systems will be provided at a level appropriate for the staff member's role and will be controlled by access levels.

11 KEY PERFORMANCE INDICATORS

- 11.1 Consistency and compliance with national standards are essential, as the Trust is measured and judged on the data they produce.
- 11.2 Data quality will be subject to internal control processes within the Trust and through external scrutiny:
- 11.3 **Internal controls:**
 - Electronic information systems and processes will have procedures developed, designed to systematically identify errors and other aspects of poor data quality.
 - Data quality reports will be locally generated regularly and considered by the appropriate monitoring leads e.g. local data quality leads or IAA which will make recommendations on data improvement.
- 11.4 Data quality reports will be routinely fed back to operational managers with advice as to corrective action to be taken such as improving processes, systems and staff training and development.
- 11.5 Audit of case records and data quality by internal auditors.
- 11.6 **External controls:**
 - Analysis of data quality reports from Secondary Use Service and the Health and Social Care Information Centre (HSCIC)
 - Queries from Commissioners and external stakeholders
 - Audits of Information

12 EQUALITY IMPACT ASSESSMENT

- 12.1 The Equality Act 2010 places a statutory duty on public bodies to have due regard in the exercise of their functions. The duty also requires public bodies to consider how the decisions they make, and the services they deliver, affect people who share equality protected characteristics and those who do not. In KMPT the culture of Equality Impact Assessment will be pursued in order to provide assurance that the Trust has carefully considered any potential negative outcomes that can occur before implementation. The Trust will monitor the implementation of the various functions/policies and refresh them in a timely manner in order to incorporate any positive changes.

13 HUMAN RIGHTS

- 13.1 The Human Rights Act 1998 sets out fundamental provisions with respect to the protection of individual human rights. These include maintaining dignity, ensuring confidentiality and protecting individuals from abuse of various kinds. Employees and volunteers of the Trust must ensure that the trust does not breach the human rights of any individual the trust comes into contact with. If you think your policy/strategy could potentially breach the right of an individual contact the legal team.

14 CONCLUSION

- 14.1 The Trust's performance, reputation and future success is dependent on the use of good quality information derived from good quality data.
- 14.2 This policy outlines the process for ensuring that the quality of data is maintained to support patient care, clinical governance, finance, workforce, and business development.
- 14.3 It will support the delivery of the Performance Strategy and Performance Management Framework to ensure that data quality is a priority for everyone in the Trust.