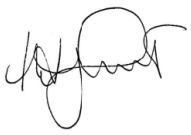
Birmingham and Solihull Mental Health NHS Foundation Trust

Information Governance Assurance Policy

Policy number and category	**IG 05**	**Information Governance**
Version number and date	**9**	**January 2021**
Ratifying committee or executive director	**Information Governance Steering Group**	
Date ratified	**March 2021**	
Next anticipated review	**March 2024**	
Executive director	**Medical Director/ Caldicott Guardian- Hilary Grant**	
Policy lead	**Head of Information Governance**	
Policy author *(if different from above)*		
Exec Sign off Signature (electronic)		
Disclosable under Freedom of Information Act 2000	**Yes**	

Policy context

Information Governance is a key part of the modern NHS. The concept of IG refers tothe way an organisation processes the information it generates through business operations Information Governance provides a way for employees to deal consistently with the different rules on how information is managed. Major legislation, this includes the Data Protection Act, NHS Confidentiality, NHS Care Record Guarantee, Information Security, NHS code of Practice, Records Management NHS Code of Practice and the Freedom of Information Act 2000.

Policy requirement (see Section 2)

- This policy supports legislation and best practice in Information Governance
- It relates to all information held in any format
- It sets the standards to be followed by all staff when handling information within the Trust
- It commits employees to specific governance requirement standards

CONTENTS

1. Introduction

1.1 Rationale

This policy describes the continued development and implementation of the robust Information Governance (IG) framework needed for the effective management and protection of organisational and personal information.

“Information Governance” describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used in the Trust are sourced, held and used appropriately, securely and legally.

‘Information Governance’ is an umbrella term for a collection of distinct but overlapping disciplines including:

- Access to information (Freedom of Information 2000, EIR Environmental Information Regulations 2004 etc)
- Confidentiality and Data Protection.
- Information Security Assurance.
- Information Quality Assurance.
- Records and Document Management (Care and Corporate).

1.2 Scope

As a provider of healthcare, the Trust carries a responsibility for handling and protecting information of many differing types. The policy covers all aspects of information within the organisation, including (but not limited to);

- Confidential Information
- Non Personal Information
- Non Confidential Information

This policy covers all aspects of information handling, including, but not limited to:

- Structured record systems – paper and electronic
- Transmission of information - fax, email, post and telephone etc….

1.3 Principles

“Information Governance” is one of the main governance arrangements within the Trust along with:

- Clinical Governance
- Risk Management
- Research Governance
- Financial Governance

“Information Governance” covers all information held by the Trust (for example – clinical, staff, financial, estates, corporate, minutes), all formats (paper and electronic) and all “information systems” used to hold that information. These systems may be purely paper-based or partially or totally electronic. The information concerned may be “owned” or required for use by the Trust and hence may be internal or external.

2. Policy

2.1 Overarching objectives of the Policy:

- Establish and maintain robust Information Governance processes conforming to the Department of Health and NHS Digital standards, best practice standards and legal requirements.
- Ensure that all practices and procedures relating to handling and holding personal and Trust corporate information are legal and conform to best and/ or recommended information and clinical practice
- Ensure appropriate awareness and training sessions are provided to all staff, and those working on behalf of the Trust, to support good Information Governance.
- Ensure that clear advice is given to service users, families and carers about how their personal information is recorded, handled, stored and shared by the Trust and its partners. Service users will be provided with guidance, available in various formats, to explain their rights, how their personal information is handled, how they can seek further information and how they can raise concerns.
- Provide clear advice and guidance to staff and ensure that they understand and apply the principles of Information Governance to their working practice in relation to protecting the confidentiality and security of personal information (for both service users and other individuals) and to ensuring the safe keeping and handling of Trust business information, ensuring compliance with appropriate legislation.
- Maintain a clear reporting structure and ensure through management action and training that all staff understand their IG requirements.
- Undertake regular reviews and audits of how information is recorded, held and used. Management and Clinical Audits will be used to identify good practice and opportunities for improvement.
- Ensure procedures are produced and regularly reviewed to monitor their effectiveness so that improvements or deterioration in information handling standards can be recognised and addressed.
- Ensure that when service developments or modifications are undertaken, a review is undertaken of all aspects of Information Governance arrangements to ensure that they are robust and effective
- Work to in-still an Information Governance culture in the Trust through increasing awareness and providing training on the key issues.
- Ensure there are robust procedures for notifying and learning from IG breaches and incidents in line with the Trust's Risk Management Policy.
- Ensure service user participation in IG developments.
- Assess performance using the Data Security and Protection Toolkit and develop and implement action plans to ensure continued improvement.

3. Corporate Procedures

As a provider of healthcare, the Trust carries a responsibility for handling and protecting information of many differing types. The policy covers all aspects of information within the organisation, including (but not limited to);

3.1 Personal Information

Much of the information the Trust creates, receives and stores is of a personal nature as it contains personal details of service users, their families or staff. The Trust must comply with legislation which regulates the holding and sharing of personal information. It is important that relevant, timely and accurate information is available to those who are involved in the care of service users, but it is also important that personal information is not shared more widely than is necessary.

3.2 Non Personal Information

The Trust also holds information which whilst not of a personal nature is still confidential. This information must be managed to ensure any commercial sensitivity is retained, as well as allowing the effective running of the organisation.

3.3 Non Confidential Information

Some information is non-confidential and may be held for the purpose of benefiting the general public. Examples include information about the Trust's services and information about mental health conditions and treatment options. The Trust and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.

3.4 Guiding Principles

There are five guiding principles that interlink which guide this IG Policy:

1. Openness and transparency
2. Legal Compliance
3. Information Security
4. Information Quality Assurance
5. Proactive use of information

3.5 Information Governance Overview

"Information Governance" covers all information held by the Trust (for example – clinical, staff, financial, estates, corporate, minutes), all formats (paper and electronic) and all "information systems" used to hold that information. These systems may be purely paper-based or partially or totally electronic. The information concerned may be "owned" or required for use by the Trust and hence may be internal or external.

3.6 Governance Requirements

The governance requirements are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Trust and ensuring that relevant information is available where and when it is needed.

Information Governance (IG) within the Trust is to be considered under 6 key themes

1. Information Governance Management
2. Confidentiality and Data Protection Assurance
3. Information Systems Security Assurance
4. Clinical Information Assurance
5. Secondary Use Assurance
6. Corporate Information Assurance

The Information Governance arrangements will underpin the Trust's strategic goals and ensure that the information needed to support and deliver their implementation is reliably available, accurate and understandable.

Implementation of robust Information Governance arrangements will deliver improvements in information handling by following the Department of Health standards (called the "HORUS model"), which requires information to be:

Held securely and confidentially
Obtained fairly and efficiently
Recorded accurately and reliably
Used effectively and ethically
Shared appropriately and lawfully

In developing this IG Policy, the Trust recognises and supports; the need for an appropriate balance between openness and confidentiality in the management and use of information. This includes:

- The principles of corporate governance and public accountability and places equal importance on the confidentiality of, and the security arrangements to safeguard, both personal information about service users, families and carers and staff and commercially sensitive information.
- The need to share service user information with partner organisations (particularly health and social care) and other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest.
- The principle that accurate, timely and relevant information is essential to deliver high quality health and social care and that it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

3.7 Openness and transparency

To ensure openness, the Trust will;

- Ensure that non-confidential information about the Trust and its services is readily and easily available through a variety of media, in line with the Trust's Freedom of Information (FOI) Publication Scheme.
- Ensure all patients and service users are aware of how their information is used and shared to support their care.
- Implement policies and procedures to ensure compliance with the Freedom of Information Act.
- Undertake or commission regular assessments and audits of its policies and arrangements for openness.
- Ensure that service users have readily and easily available access to information relating to their own care, their options for treatment and their rights as service users.
- Procedures will be in place detailing how this process will be managed and made available to service users.
- Have clear procedures and arrangements for liaison with the press and broadcasting media.
- Have clear procedures and arrangements for handling queries from service users and the public.

3.8 Legal Compliance

To ensure Legal Compliance, the Trust and particularly the Information Governance Assurance structure will;

- Regard all identifiable personal information relating to service users as confidential.
- Establish and maintain policies and protocols for the controlled and appropriate sharing of service user information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

- Undertake or commission annual assessments and audits of its compliance with legal requirements.
- Regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- Establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law duty of confidentiality and all associated guidance.
- Establish and maintain policies to ensure compliance with the Freedom of Information Act and Environmental Information Regulations.

3.9 Information Systems Security and Legal Compliance

To ensure that appropriate and legal compliant Information Systems Security exists, the Trust and particularly the Information Governance Assurance structure will;

- Establish, maintain and develop its Information Systems Security Policy, along with respective procedures for effective policing and secure management of all its information assets, resources and IT systems.
- Undertake and/or commission annual assessments and audits of its information and IT security arrangements in-line with the said policy.
- Promotes effective confidentiality and security practice, to ensure all permanent/temporary; contracted staff and third party associates of the trust adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation.
- Establish, maintain and develop appropriate policies and procedures for the safe and secure transmission of all types of data using security measures (such as encryption) where required.
- Establish, maintain and develop appropriate policing, incident reporting procedures and monitoring and investigations of all instances, actual and/or potential, along with any reported breaches of confidentiality and security.
- Implement staff roles with specific responsibility for managing the security of information within systems.

3.10 Information Quality Assurance

To ensure Information Quality Assurance, for both clinical and business information, the Trust and particularly the Information Governance Assurance structure will;

- Establish, maintain and develop policies and procedures for information quality assurance and the effective management of records.
- Undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Ensure that key service user data is accurately recorded and maintained,

including regular cross-checking against source data.
- Ensure that managers are required to take ownership of, and seek to improve; the quality of information within their services and that information quality is assured at the point of collection.
- Ensure that data standards are set through clear and consistent definition of data items, in accordance with national standards.
- Promote information quality and effective records management through policies, procedures/user manuals and training.

3.11 Proactive Use of Information

To ensure proactive use of information, the Trust, and particularly the Information Governance Assurance structure will;

- Ensure information systems hold the information required to support clinical practice and operational management.
- Develop information systems and reporting processes which support effective performance management and monitoring.
- Develop information management awareness and training programmes to support managers in using information to manage and develop services.
- Support clinical, corporate, financial and research governance requirements.
- Promote an information culture and expectation of informed, evidence-based decision making. Ensure that, where appropriate and subject to confidentiality constraints, information is shared with other NHS, social care and partner organisations in order to support patient care.

3.12 Implementation of IG Strategy

The implementation of this IG Strategy will ensure that the Trust and its staff handle and manage information in a consistent way. This is anticipated to lead to;

- Improvements in information handling activities.
- Reduction in numbers of IG incidents and complaints.
- Increased service user confidence in the NHS, the Trust and its staff.

3.13 Information Governance Framework

Information Governance provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal and Trust information, ensuring.

- Compliance with the law and professional standards.
- Implementation of Department of Health advice and guidance.
- Year on year improvement.

3.14 Associated Trust Policies

- Confidentiality Policy
- Corporate Records Management Policy
- Information, Communications and Technology Policy
- Data Quality Policy
- Freedom of Information Policy
- Care (Health) Records Management Policy

3.15. Information Governance Reporting Structure

3.15.1 Information Governance Infrastructure

The Information Governance infrastructure consists of a Steering Group accountable to the Trust Board. There will be 3 working groups which undertake the detailed work;, these are led by a senior manager responsible for the majority of the work topic.

3.15.2 Responsibilities of the Information Governance Steering Group

The Trust Information Governance Steering Group (IGSG) is responsible to act on behalf of Trust Board for;

- Overseeing the implementation of this strategy
- The annual review of this strategy
- The development, approval and implementation of the associated policies and procedures in relation to the 6 working groups
- Reviewing and signing off the IG work programme
  Ensuring the accurate and complete completion, review and sign off of the Data Security and Protection Toolkit Assessment to a satisfactory standard.

3.15.3 Information Governance Steering Group Progress Reporting

The IGSG will report progress yearly to the Trust Board and to Integrated Quality Committee on a quarterly basis

3.15.4 Information Governance Working Groups

There are 5 working groups responsible for IG;

- Information Governance Steering Group (senior membership)
- Data Protection Impact Assessment Virtual Approval Group
- InformationGovernance and Security Assurance Group
- Secondary Use Assurance Group
- Information Asset Owners Workshop

3.15.5 Membership of the Information Governance Steering Group

The membership of the IGSG is;

- Executive Director of Finance(Senior Information Risk Owner)
- Medical Director (Caldicott Guardian) - Chair
- Deputy Medical Director (Deputy Caldicott Guardian)
- Chairs of IG working groups
- Head of Information Governance
- Head of Care Records and Clinical Coding
- Clinical Chief Information Officer
- Associate Director of Performance & Information (Deputy SIRO)
- Associate Director of Governance

Other staff may be co-opted as required.

3.16. Strategy Implementation

3.16.1 IGSG Role

The IGSG will monitor the implementation of this policy and its associated work programmes, through regular meetings and through the IG sub groups.

3.16.2 Data Security and Protection Toolkit

All Trusts are mandated to complete a self-assessment of their IG performance using the NHS Digital Data Security and Protection Toolkit. This is an on-line self assessment tool which is updated annually. The self-assessment score is used as one of the sources of information and evidence by the Care Quality Commission when assessing compliance with Standards for Better Health, self improvement reviews etc.

The Information Governance standards are based on generally accepted definitions of good practice in relation to Information Governance and inter-link with other recommendations and standards such as those in Standards for Better Health, CNST and the Data Protection Act 2018, Computer Misuse Act 1990, etc..

3.16.3 IG Working Group Responsibilities

The responsibilities of each IG working group are to:

- Undertake a baseline assessment of their current position in relation to their IG standards (using the self assessment toolkit)
- Agree an annual work programme to ensure a year on year improvement in performance
- Ensure the timely development of strategies, policies, procedures etc required for Information Governance
- Identify resources required for implementation
- Monitor progress made
- Report on progress, incidents and issues to the IGSG in advance of the nationally mandated submission dates
- Assess their own performance against the Data Security and Protection toolkit in line with national requirements and timescales.
- Complete the self assessment tool kit in line with the nationally mandated submission requirements

3.16.4 IG Strategy Review

The Chairs of the working groups are responsible for determining the membership of these groups and the frequency and format of meetings, which may be incorporated into other formal management groups if appropriate.

3.17. Incident Management

Trust staff are required to follow an incident reporting process to ensure the Trust can regularly review incidents and learn from near misses and reported incidents. Please refer to all Trust Procedures in place.

The Trust is required to report incidents defined as ‘serious’ to the Information Commissioners Office where the incident meets criteria as defined in the Information Commissioner Incident Reporting Tool.

3.18. Year on Year Improvement Plan and Assessment

An assessment of compliance with requirements, within the Data Security and Protection Toolkit will be undertaken each year. Annual reports and proposed action/ development plans will be presented to relevant groups and Trust Board for approval prior to final submission. Internal audits will be carried out throughout the Trust, so to continually monitor that staff’s compliance is being maintained.

3.19. IG Training

The Trust will provide comprehensive training to its staff to allow them to meet their Information Governance requirements. Where specific training is required it will be promoted so staff can meet their obligations. These could be in a variety of formats (e-learning, external courses etc)

All staff will be required to attend, as part of their induction, a training session on Information Governance. Additional statutory/ mandatory training will then be required to be completed using the e-learning IG training module on an annual basis. Managers will be responsible for ensuring staff are compliant as part of the Trust's fundamental training requirements.

The Caldicott Guardian and Senior Information Risk Owner (SIRO) will be required to complete additional specialist refresher training every two years unless there is a change to data protection legislation during the two year period which would require the training to be completed earlier.

3.20. Conclusion

The ongoing development and maintenance of the Information Governance strategy, infrastructure and action plans will ensure that all types of information is more effectively managed and proactively utilised at Birmingham & Solihull Mental Health Foundation Trust.

4. Key roles and Responsibilities

Post(s)	Responsibilities	Ref
Chief Executive	As the Accountable Officer, they have the overall responsibility for Information Governance within the Trust	
Trust Board	The Board is responsible for ensuring that Information Governance is addressed at a strategic level and assurance provided via the Trust Board sub-committee Integrated Quality Committee. The named Executive Directors on the Trust Board with responsibility for Information Governance is the Medical Director and Executive Director of Finance.	
Executive Team	Are responsible for Information Governance at an operational level and are accountable to the Board. The Executive Team will ensure there is an	

	adequate level of resources and expertise to deal with the range of issues that arise across the Information Governance function	
Executive Medical Director	The Executive Medical Director is also the Caldicott Guardian has overall responsibility for ensuring information relating to patients and the users of the services is used confidentially and handled with the appropriate safeguards.	
Executive Director of Finance	The Executive Director of Finance is also the Senior Information Risk Owner (SIRO) which is a mandated role and has overall responsibility for managing information risk across the Trust. They are also the owner of the Trusts Information Risk and Issues Register. The SIRO is a member of the Executive team and is assisted by; • The Trust's Data Protection Officer- the Head of IG; • The Trust's Deputy SIRO • The Trust's Information Systems Security Officer is the Head of IT; • The Head of Information Governance An Information Asset Owner will be identified for each of the Trust's critical information assets.	
Information Security Managers	The Head of Technical Services and Information Security Officer are mandated roles and will lead the Information Services and Information Security Teams. They are accountable to the Deputy SIRO. They have day to day operational responsibility for all aspects of information security (including personnel and physical security where it has the potential to impact upon information security) and will work with the SIRO & Deputy SIRO to ensure information risk is managed appropriately	

Head of Information Governance / Data Protection Officer	This role will lead the Information Governance agenda for the Trust and is accountable to the Associate Director of Performance and Information, Deputy SIRO. They will have day to day operational responsibility for all aspects of Information Governance (except information security and data quality although they will provide assistance where required). The Head of Information Governance also acts as the Trust's Data Protection Officer	
Information Asset Owner	This is a mandated role and will be the senior individual involved in running the relevant business area. The Information Asset Owners are responsible for ensuring adherence to the protective marking system and records retention schedule.	
All Staff	Staff are responsible for ensuring that they comply with the Information Governance framework and will ensure that all work programmes acknowledge the requirements of the framework.	

5. Development and Consultation Process

5.1 Policy Review

The IGSG will review this strategy bi-annually or in response to any significant changes to mandatory requirements, national NHS or partner organisations guidance or as a result of significant Information Governance breaches or incidents.

5.2 Consultation Summary

Consultation summary	
Date policy issued for consultation	January 2021
Number of versions produced for consultation	1
Committees / meetings where policy formally discussed	**Date(s)**
IGSG	9th September 2020
PDMG	February 2021

Where received	Summary of feedback	Actions / Response

6. Reference Documents

6.1 National reference documents

- General Data Protection Regulations and Working Party 29 guidance
- Public Records Acts 1958 and 1967
- Freedom of Information Act 2000 (FOIA)
- Records Management: NHS code of practice Parts 1 and 2
    - http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747
- NHS Digital Data Security and Information Toolkit
- Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000; website:
    - http://www.nationalarchives.gov.uk/information-management/legislation/section-46.htm
- Computer Misuse Act 1990

6.2 Relevant Trust policies/ sources of guidance:

(Please note: this list is not exhaustive)

- Freedom of Information & Environmental Information Regulations - CG 08
- Corporate Records Management Policy
- The Management of Intellectual Property - CG 07
- Care Records Management - C 12
- Confidentiality Policy- IG 01
- Information Communications and Technology Policy- IG 02
- Information Systems and Information Asset Owners Guidelines
- Data Quality - IG 03
- Policy Development and Management CG 01
- Volunteer Policy - HR 25 } and other HR policies
- Employment of Service Users - HR 29 }
- Health & Safety Policies
- BSMHFT Energy and Transport policies
- E-mail, Internet Access and Data Network Guidelines
- Use by staff of Mobile Telephones, PDA's and other Handheld Electronic Technology
- Information Asset Owners Procedures
- System Level Security Policy

7. Bibliography

7.1 General

- General Data Protection Regulations – Working Party 29 and ICO available guidance

- The Data Protection Act 2018 (DPA)
  - http://www.legislation.gov.uk/ukpga/1998/29
- The Freedom of Information Act 2000 (FOIA)
  - http://www.legislation.gov.uk/ukpga/2000/36/contents
- The Environmental Information Regulations 2004 (EIRs)
  (Note: The combined effect of the above legislation is to create an access to information regime. The DPA facilitates access to personal information of which the applicant is the subject; the FOIA enables public access to corporate information and the EIRs enable public access to environmental information.)
- Various British Standards of which the following is a selection:
  - BS 4783 Storage, transportation and maintenance of media for use in data processing and information storage
  - BS 17799 Code of practice for information security management
  - BS ISO 15489 Information and Documentation - Records Management
  - BSI DISC PD 0008 Code of practice for legal admissibility and evidential weight of information stored on electronic document management systems
  - BSI DISC PD0010 Principles of good practice for information management
  - BS 8470 Secure destruction of confidential material code of practice

7.2 Other relevant legislation / sources of guidance:

- Health and Social Care Act 2008
- Human Rights Act 1998
- The National Archives website: http://www.nationalarchives.gov.uk/
- Department of Health's website: http://www.dh.gov.uk/en/index.htm

Note: This is not a comprehensive list of all standards, guidelines and legislation

8. Glossary / Definitions

The following terms/acronyms are used within this document.

The Trust	Birmingham & Solihull Mental Health Foundation Trust
IGSG	Information Governance Steering Group
IG	Information Governance
NHSIA	National Health Service Information Authority
NCRS	NHS Care Records Service
C4H	Connecting for Health
NPfIT	National Program for Information Technology
SIRO	Senior Information Risk Owner
IAO	Information Asset Owner

9. Audit and Assurance

Element to be monitored	Lead	Tool	Frequency	Reporting Arrangements

Data Security and Protection Toolkit	Head of IG	Verbal and Written Reports	Bi-monthly	IGSG
IG training	Head of IG	InSight report	Bi-monthly	IGSG
Incident Management	Head of IG	Eclipse	Daily as required	IGSG

10. Appendices

Appendix 1 Equality Impact Assessment
Appendix 2: IG Hierarchy chart (p.17)

Title of Proposal	**Information Governance Assurance Policy, Confidentiality Policy and Access to Information Policy**		
Person Completing this proposal	**Kirstie Macmillan**	**Role or title**	**Head of Information Governance**
Division	**Corporate**	**Service Area**	**Performance and Information**
Date Started	**January 2021**	**Date completed**	**January 2021**

Main purpose and aims of the proposal and how it fits in with the wider strategic aims and objectives of the organisation.

These policies identify how the Trust will uphold data subjects rights and expectations in regards to data protection and associated principles and legislation.

Who will benefit from the proposal?

All service users and members of staff

Impacts on different Personal Protected Characteristics – *Helpful Questions:*

Does this proposal promote equality of opportunity? *Eliminate discrimination?* *Eliminate harassment?* *Eliminate victimisation?*	*Promote good community relations?* *Promote positive attitudes towards disabled people?* *Consider more favourable treatment of disabled people?* *Promote involvement and consultation?* *Protect and promote human rights?*

Please click in the relevant impact box or leave blank if you feel there is no particular impact.

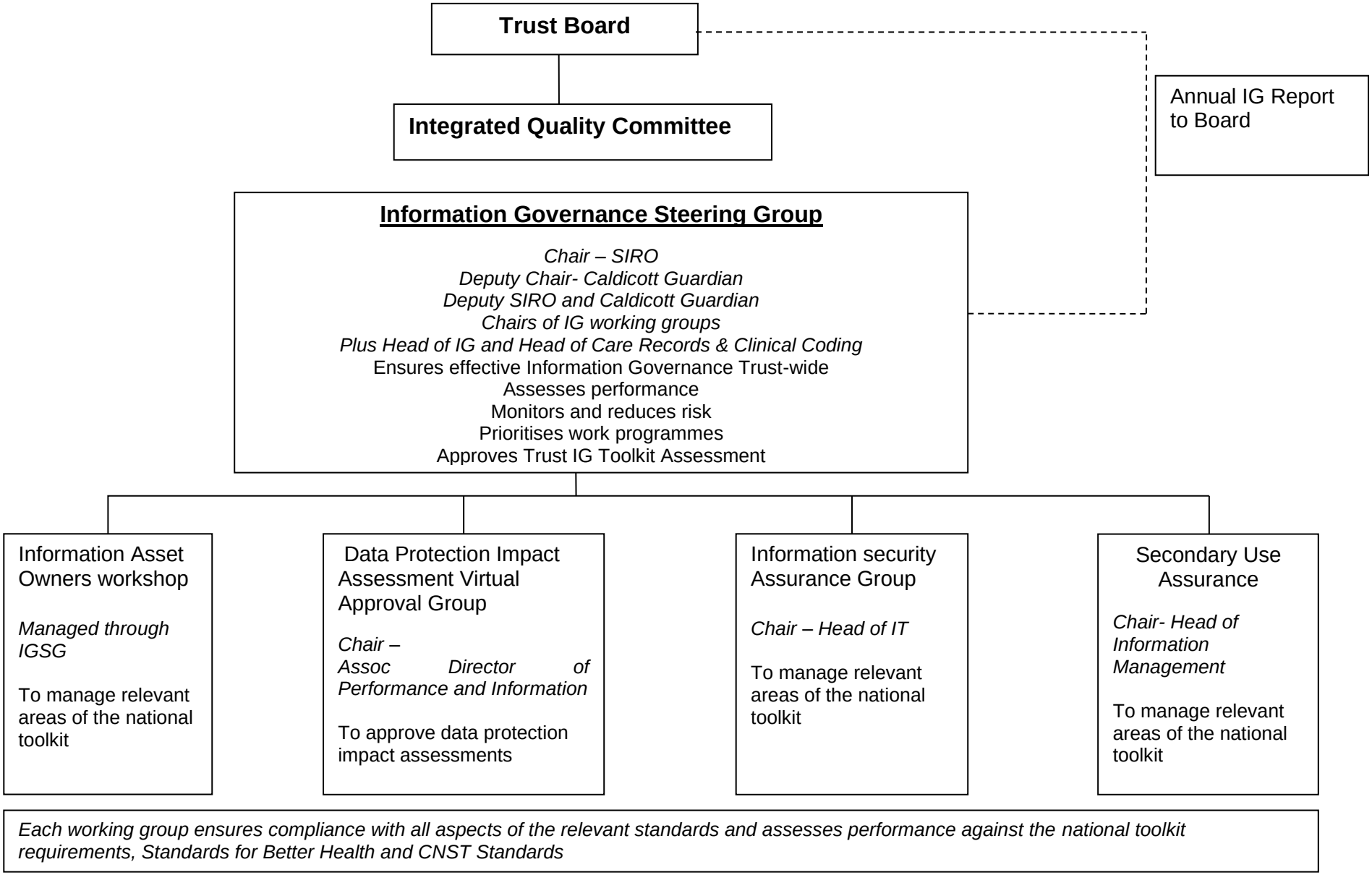
Personal Protected Characteristic	No/Minimum Impact	Negative Impact	Positive Impact	Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.
Age				*These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection*
Including children and people over 65				

Is it easy for someone of any age to find out about your service or access your proposal? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability				***These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection***
Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				
Gender				***These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection***
This can include male and female or someone who has completed the gender reassignment process from one sex to another Do you have flexible working arrangements for either sex? Is it easier for either men or women to access your proposal?				
Marriage or Civil Partnerships				***These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection***
People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?				
Pregnancy or Maternity				***These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection***
This includes women having a baby and women just after they have had a baby Does your service accommodate the needs of expectant and postnatal mothers both as staff and service users? Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?				
Race or Ethnicity				***These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection***
Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees What training does staff have to respond to the cultural needs of different ethnic groups? What arrangements are in place to communicate with people who do not have English as a first language?				

Religion or Belief				**These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection**
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? When organising events – Do you take necessary steps to make sure that spiritual requirements are met?				
Sexual Orientation				**These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection**
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples? Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?				
Transgender or Gender Reassignment				**These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection**
This will include people who are in the process of or in a care pathway changing from one gender to another Have you considered the possible needs of transgender staff and service users in the development of your proposal or service?				
Human Rights				**These policies provide guidance for staff on how to uphold service users, carer's and stakeholders rights under data protection**
Affecting someone's right to Life, Dignity and Respect? Caring for other people or protecting them from danger? The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)				
	Yes	**No**		
What do you consider the level of negative impact to be?	**High Impact**	**Medium Impact**	**Low Impact**	**No Impact**

If the impact could be discriminatory in law, please contact the **Equality and Diversity Lead** immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required. If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the **Equality and Diversity Lead** before proceeding. If the proposal does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the **Equality and Diversity Lead.**
Action Planning:
How could you minimise or remove any negative impact identified even if this is of low significance?
These policies ensure that the Trust meets its legal obligations under Data Protection law.
How will any impact or planned actions be monitored and reviewed?
Trust adherence to the policies will be monitored via planned information governance audits.
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.
Please save and keep one copy and then send a copy with a copy of the proposal to the Senior Equality and Diversity Lead at hr.support@bsmhft.nhs.uk. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis.

Appendix 2


Trust Board
Integrated Quality Committee
Annual IG Report to Board
Information Governance Steering Group
Chair – SIRO
Deputy Chair- Caldicott Guardian
Deputy SIRO and Caldicott Guardian
Chairs of IG working groups
Plus Head of IG and Head of Care Records & Clinical Coding
Ensures effective Information Governance Trust-wide
Assesses performance
Monitors and reduces risk
Prioritises work programmes
Approves Trust IG Toolkit Assessment
Information Asset Owners workshop
Managed through IGSG
To manage relevant areas of the national toolkit
Data Protection Impact Assessment Virtual Approval Group
Chair – Assoc Director of Performance and Information
To approve data protection impact assessments
Information security Assurance Group
Chair – Head of IT
To manage relevant areas of the national toolkit
Secondary Use Assurance
Chair- Head of Information Management
To manage relevant areas of the national toolkit
Each working group ensures compliance with all aspects of the relevant standards and assesses performance against the national toolkit requirements, Standards for Better Health and CNST Standards