NHS
South Tees
Clinical Commissioning Group

Information Governance and Information Risk Policy

Ratified	Approved
Status	Final
Issued	November 2017
Approved By	Governance and Risk Committee
Consultation	Governance and Risk Committee NECS IG Team
Equality Impact Assessment	Completed
Distribution	All Staff
Date Amended following initial ratification	July 2018
Implementation Date	July 2018
Planned Review Date	July 2020
Version	2.2
Author	Senior Governance Officer (IG), NHS North of England Commissioning Support Unit
Reference No	IG03

Policy Validity Statement
This policy is due for review on the date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

Version Control

Version	Release Date	Author	Update comments
V1	April 2013	NECS	
V2	July 2014	Liane Cotterill	Review and update
V2.1	October 2017	Liane Cotterill	Review and update to include GDPR
V2.2	May 2018	Alan Clement	Updated following publication of the Data Protection Act 2018

Approval

Role	Name	Date
Approval (1)	Governing Body	April 2013
Approval (2)	Governance & Risk Committee	October 2014
Approval (2.1)	Governance & Risk Committee	November 2017
Approval (2.2)	Governance & Risk Committee	July 2018

Review

This document will be reviewed twelve months from its issue date and no longer than 3 years after its first review.

.

Contents

1. Introduction

The CCG aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

Information is a vital asset, both in terms of the management of health and social care for individual patients/service users and the efficient management of services and resources. It plays a key part in governance, service planning and performance management.

Information risk management is an essential component of information governance and is an integral part of good management practice. The intent is to embed information risk management in a practical way into business processes and functions.

Information risk must be managed in a robust way within work areas and not be seen as something that is the sole responsibility of IT or IG staff. A structured approach is needed, building upon the existing information governance framework and this approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

It is therefore of paramount importance to ensure that information is efficiently managed including information risk, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management. Information Governance (IG) is the means of providing this governance framework, and currently includes the following legislation and guidance:

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records Act 1990
- Department of Health Records Management: NHS Code of Practice
- Computer Misuse Act 1990
- NHS Confidentiality Code of Practice
- Common Law Duty of Confidentiality
- Fraud Act 2006
- Further guidance on information governance legislation can be found in the Department of Health NHS Information Governance Guidance on Legal and Professional obligations.

The Framework sets out an overview of how the organisation is addressing the IG Agenda and the approach taken to ensure robust management of information. There are two key components underpinning the IG Framework;

- IG Policy which outlines the objective for information governance
- IG Strategy which details overall plan arising from a baseline assessment against the requirements set out in the NHS Digital Data Protection and Security Toolkit.

The Data Protection and Security Toolkit consists of a series of evidence based requirements against which an organisation's current and planned attainment levels can be monitored. The organisation is required to complete an annual self-assessment against the Toolkit. The CCG Toolkit is broken down into ten National Data Guardian Standards:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems
- IT Protection
- Accountable Suppliers

1.1 Status

This policy is an Information Governance policy.

1.2 Purpose and scope

The purpose of this document is to present an Information Governance Policy & Information Risk Policy for the organisation. This sets out the organisation's commitment to the security, information risk management, confidentiality and quality of information. It also details how information governance and information risk will be managed within the organisation.

This policy is applicable to all employees, agents and contractors working for, or supplying services to the organisation. However, it is recognised that primary care practitioners are also part of the organisation and as such this policy is offered for use by them to adapt to their own practices and organisations as appropriate. The contact for the policy (see Useful Contacts Section) is available to offer help and support to primary care practitioners who wish to use and implement this policy.

2. Definitions

The following terms are used in this document:

2.1 **Personal information** is factual information or expressions of opinion which relate to an individual who can be identified from that information or in conjunction with any other information coming into possession of the data holder. This also includes information gleaned from a professional opinion, which may rely on other information obtained. Personal information includes name, address, date of birth or any other unique identifiers such as NHS Number, Hospital Number, National Insurance Number, etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode, date of birth etc.

2.2 **Sensitive information** also known as 'Special Category Data' as set out in the DPA 2018 is any information about a person relating to their;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Biometric Data
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed

This type of data is subject to more stringent conditions on their processing when compared to 'personal information' (See 2.1).

2.3 **Information risk** is the chance of something happening to the information which will have an impact upon the objectives, personal safety and security of the organisation. Risk is determined in terms of consequence and likelihood and should be managed alongside other organisational risks and should be considered a fundamental component of effective information governance.

2.4 **Information Risk Management** is the culture, processes and structures that are directed towards the effective management of opportunities and adverse effects to information assets.

2.5 **Information assets** come in many shapes and forms and include:

- **Personal information** e.g. content within databases, archive and back up data, audit data, paper records (health, social care and staff records)
- **Software** e.g. application and system software, data encryption utilities, development and maintenance tools
- **Hardware** e.g. PCs, laptops, USB sticks, PDA
- **System/process documentation** e.g. system information and documentation, manual and training materials, contracts, business continuity plans, policies etc.

2.6 **Information Asset Register** is a record of all information assets along with the associated Information Asset Owner of each asset. Having an up to date and accurate IAR is a requirement under GDPR.

2.7 **Privacy by Design** means any action that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that any department that processes personal data, must ensure that privacy is built in to the whole life cycle of the process.

2.8 **Privacy by Default** means that once a product, process, or service has been introduced, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user should only be kept for the amount of time necessary to provide the service.

2.9 **Data Protection Impact Assessment** (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must complete a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing

3. The Principles of Information Governance

3.1 Overview

3.1.1 There are a number of underlying principles governing Information Governance. An Information Governance Strategy will detail how these principles will be embedded throughout the organisation.

3.1.2 These principles can be divided into the different areas of information governance.

3.2 Information Governance Management

- There is a commitment to establish and maintain robust operational and management accountability structures, assign appropriate resources and dedicated staff to ensure IG issues are dealt with appropriately, effectively and at levels within the organisation.
- There should be proactive use of information within and between the organisation, other NHS, and partner organisations to support patient/service user care as determined by law, statute and best practice.
- There is a need for an appropriate balance between openness and confidentiality in the management and use of information.
- There is a commitment to improving staff understanding of their responsibilities around information governance at a level relevant to their role.
- There is a legal requirement to consider privacy by design when implementing any new or changed system or service being implemented.
- There is a dedicated Information Governance component in the appropriate budget within the organisation.

3.3 Confidentiality and Data Protection Assurance

- There is a need to share patient/service user information with other health organisations and other non-health agencies in a controlled manner consistent with the interests of the patient/service user and, in some circumstances, the public interest.
- There should be effective arrangements to ensure confidentiality and security of personal and other sensitive information.
- There is a legal requirement to undertake Data Protection Impact Assessments for new processes, systems, projects etc.

3.4 Information Security Assurance

- There is a commitment to ensuring the security of all personal information held by the organisation through the implementation of

policies, procedures and processes to ensure the confidentiality, integrity and availability of information
- There is a commitment to the implementation of security monitoring and audit processes to ensure compliance with key policy and procedures.
- There is a need legal requirement to consider privacy by default when implementing systems and technologies.

3.5 Corporate Information Assurance

- There is a commitment to making non-confidential information widely available in line with responsibilities under FOI Act 2000 to ensure openness.
- There is a need for effective management of corporate paper and electronic records

.

3.6 Clinical Information Assurance

- There is a need for accurate, timely and relevant information in order to deliver the highest quality health and social care.
- There is a commitment to improving records management for care purposes in keeping with professional, legislative and statutory records management requirements

3.7 Secondary Use Assurance

- There is a commitment to developing quality data to support non-direct care related purposes (planning, commissioning, public health, finance)
- There is a commitment to improving data quality through the use of local and national benchmarking

4. Managing Information Risk

4.1 Introduction

4.1.1 The organisation places high importance on minimising information risk and safeguarding the interest of patients, staff and the organisation.

4.1.2 Information risk is inherent in all organisational activities and everyone working for, or on behalf of the organisation, has a responsibility to continuously manage information risk. The aim of information risk management is to provide the means to identify, prioritise and manage the risks involved in all of the organisation's activities.

4.2 Information Risk Management Assurance Framework

4.2.1 Information Risk Management Assurance Framework aims to:

- Protect patients, staff and the organisation from information risks where the likelihood of occurrence and the consequences are significant.
- Support the strategic approach to the risk management framework in which information risks will be identified, considered and addressed in the approval, review and control processes.
- Use the risk assessment methodology (risk matrix) to assess information risks e.g. threats to information.
- Encourage pro-active rather than re-active information risk management.
- Contribute to the quality of decision making throughout the organisation by supporting robust information.
- Meet legal or statutory requirements.
- Assist in safeguarding the organisation's information assets.

4.3 Assessment of Information Risk

4.3.1 The organisation will assess information risk in a number of ways, which will include the following;

- Routine review of flows of personal information to ensure any risks identified with these flows are mitigated, including ensuring appropriate controls are in place for data transferred outside the EEA.

- The organisation's risk management procedures provide clear guidance as to the way in which information risks and incidents are identified, assessed and managed across the organisation, and how the IG Risk Register supports this process. Investigating and learning from incidents will support the organisation in understanding the real level of risk being experienced and in adjusting the controls in place.

- Undertaking Data Protection Impact Assessments and System Security Level risk assessments as methods through which information assets can be risk assessed and assured they comply with the required standards.

5. Duties and Responsibilities

Council of Members	The Council of Members has delegated responsibility to the Governing Body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Chief Officer	The Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements. The Chief Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level and handled in a similar manner to other major risks such as financial. The Chief Officer will identify additional resources where necessary to support the IG agenda.
Governance and Risk Committee (responsible for IG)	The Governance and Risk Committee has a responsibility to: • Develop the Information Governance agenda across the organisation. • Monitor the organisation's progress in this area using the NHS Digital Information Governance Toolkit. • Ensure action plans are developed in each of the different areas of IG to meet the IG standards and requirements. • Carry out specific pieces of work in accordance with the action plans. • Ensure IG Policies and procedures are developed, implemented and reviewed appropriately. • Ensure all risks and incidents associated with IG and Information Risk are identified, logged, actioned and monitored routinely.
Information Governance Team (CSU)	The Information Governance Team has a responsibility to: • Provide information governance support to staff in the organisation. • Co-ordinate different areas of information governance and ensure progress against key standards and requirements. • In collaboration with IT, develop, implement and monitor information security across the organisation. • To support the CCG in evidence collation, upload and publication of the IG Toolkit.

Freedom of Information (FOI) Lead(CSU)	Freedom of Information(FOI) Lead (CSU); has a responsibility to: • Appropriate policies and procedures relating to FOI are developed and available to staff. • Ensure the "Guide to Information" (formerly Publication Scheme) is kept up to date and available on the public website. • Ensure all FOI requests and exemptions are processed in an appropriately, timely manner. • Investigations are dealt with appropriately.
CSU Staff	Whilst working on behalf of the CCG, CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the CCG, however they will continue to be governed by all policies and procedures.
Caldicott Guardian	The Caldicott Guardian has a responsibility to: • Ensure the organisation satisfies the highest confidentiality standards. • Advise on lawful and ethical processing of information. • Ensure appropriate processes and procedures are established to enable the organisation to act in accordance with the Caldicott principles. • Represent and champion information governance and report issues at Governing Body/Senior Management Team level. • Take a key role in ensuring standards of confidentiality in relation to the National Programme for IT. • Act as signatory for high level information sharing agreements.
Senior Information Risk Owner (SIRO)	The Senior Information Risk Owner (SIRO) has a responsibility to: • Oversee the development of an Information Governance & Information Risk Policy and Strategy and its implementation. • Take ownership of risk assessment process for information risk. • Review and agree action in respect of identified information risks. • Ensure that the Organisation approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff. • Provide a focal point for the resolution and/or discussion of information risk issues. • Ensure the Governing Body is adequately briefed on information risk issues. • Successfully complete strategic information risk management training at least annually.

Information Asset Owners	Information Asset Owners (IAOs) are responsible for: • Liaising with records management/IG leads to ensure that records management practices are in line with the guidance and protocols on confidentiality. • Ensuring appropriate record audits are undertaken. • Ensuring appropriate information governance /confidentiality clauses are in third party contracts relating to records management such as secondary storage, scanning companies before using the company. • Ensuring appropriate consideration is given to records management within business continuity plans. • Ensuring they obtain appropriate certifications of destruction. • Investigate and take relevant action on any potential breaches of this policy supported by other applicable staff in line with existing procedures.
Information Asset Administrators (IAA)	Information Asset Administrators (IAA) support the IAO to ensure that policies and procedures are followed, recognise actual and potential security incidents, consult the appropriate IAO on incident management, and ensure that information asset registers are accurate and up to date.
Line Managers	Line managers have a responsibility to: • Ensure all current, new and temporary staff are instructed in their responsibilities in relation to the Information Governance and Information Risk Policy & Strategy and related policies and procedures, and work in a manner consistent with this policy. • Ensure staff are appropriately trained in information governance in line with the requirements of their post. • In certain circumstances, to support equality & diversity, line managers will need to consider individual requirements of staff to support good practice in complying with this policy. • Investigate and take relevant action on any potential breaches of this policy supported by risk management leads and IG Team in line with existing procedures.

All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided. • Adhere to the IG and Information Risk Policy and Strategy and all related policies and procedures and relevant legislation. • Conduct themselves in accordance with the IG section in the staff employment contract and within the Confidentiality Code of Conduct (appendix to Confidentiality and Data Protection Policy). • Be aware that failure to comply with this Policy may result in disciplinary action being taken. • Undertake mandatory IG training as part of induction and annual training. • Undertake IG training in line with the requirements of their role. • Bring to their line manager areas of concern regarding information governance and information risk. • Report incidents through the organisation's incident reporting process.

6. Implementation

6.1 This policy will be available to all staff for use in relation to the specific function of the policy.

6.2 All managers are responsible for ensuring that relevant staff within the CCG have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

6.3 This policy will be implemented in the following ways:

- Mandatory Data Security Awareness training
- Regular communications to staff on new Information Governance policies and procedures
- Guidance and access to policies and procedures
- The Information Governance Team will be the key contact point for staff support within the organisation
- Regular audit of information governance processes undertaken in line with information governance policy and procedures in key areas i.e. records management, confidentiality, information security, freedom of information and data quality
- Monitoring of information governance processes through the Data Protection and Security Toolkit.

7. Training Implications

The Governance and Risk Committee has ultimate responsibility for ensuring that the necessary training or education needs and methods required to implement the policy or procedure(s) are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

8. Related Documents

8.1 Legislation and statutory requirements

- Cabinet Office (1990) *Computer Misuse Act 1990*. London. HMSO
- Cabinet Office (2018) *Data Protection Act 2018* London. HMSO.
- Cabinet Office (1990) *Access to Health Records Act 1990.* London. HMSO.
- Cabinet Office (2000) *Freedom of Information Act 2000*. London. HMSO.
- Cabinet Office (2004) *Environmental Information Regulations 2004*. London. HMSO.
- Cabinet Office (2006) *Fraud Act 2006*. London. HMSO
- EU General Data Protection Regulations 2016

8.2 Best practice recommendations

- Department of Health's Records Management Code of Practice for Health and Social Care 2016.
- NHS Confidentiality Code of Practice
- Common Law Duty of Confidentiality

9. Monitoring, Review and Archiving

9.1 Monitoring

9.1.1 The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

9.1.2 All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for information governance.

9.1.3 Failure to follow this policy and related information governance policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

9.1.4 Different methods will be used for monitoring different aspects of information governance including:

- Monitoring of information governance processes through the Data Protection and Security Toolkit.
- Audit of information flows to ensure confidential information is being transferred securely and in order to minimise information risk.
- Regular audit of information governance processes undertaken in line with information governance policy and procedures in key areas i.e. records management, confidentiality, information security, freedom of information, data quality.
- Action plans resulting from data protection impact assessments and system level security assessments are appropriately implemented to minimise information risk.
- The organisation will, in conjunction with the internal and external audit, identify any areas for improvement of IG and information risk and development and agree appropriate actions plans.

9.2 Review

9.2.1 The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

9.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

9.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

9.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with Department of Health's Records Management Code of Practice for Health and Social Care 2016.

10. Equality Analysis

An equality impact assessment has been completed:

Partners in improving local health

North of England Commissioning Support

Introduction - Equality Impact Assessment

An Equality Impact Assessment (EIA) is a process of analysing a new or existing service, policy or process. The aim is to identify what is the (likely) effect of implementation for different groups within the community (including patients, public and staff).

We need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- Advance equality of opportunity between people who share a protected characteristic and those who do not
- Foster good relations between people who share a protected characteristic and those who do not

This is the law. In simple terms it means thinking about how some people might be excluded from what we are offering.

The way in which we organise things, or the assumptions we make, may mean that they cannot join in or if they do, it will not really work for them.

It's good practice to think of all reasons why people may be excluded, not just the ones covered by the law. Think about people who may be suffering from socio-economic deprivation or the challenges facing carers for example.

This will not only ensure legal compliance, but also help to ensure that services best support the healthcare needs of the local population.

Think of it as simply providing great customer service to everyone.

As a manager or someone who is involved in a service, policy, or process development, you are required to complete an Equality Impact Assessment using this toolkit.

Policy	A written statement of intent describing the broad approach or course of action the Trust is taking with a particular service or issue.
Service	A system or organisation that provides for a public need.
Process	Any of a group of related actions contributing to a larger action.

STEP 1 - EVIDENCE GATHERING

Name of person completing EIA:	**Liane Cotterill**
Title of service/policy/process:	**Information Governance & Information Risk Policy**
Existing: √ New/proposed: □ Changed:	
What are the intended outcomes of this policy/service/process? Include outline of objectives and aims	
This policy sets out the organisation's commitment to the security, information risk management, confidentiality and quality of information. It also details how information governance and information risk will be managed within the organisation. The policy compliments other Information Governance policies.	

Who will be affected by this policy/service /process? (please tick)

□ **Consultants** □ **Nurses** □ **Doctors**
√ **Staff members** □ **Patients** □ **Public**
□ **Other**

If other please state:

What is your source of feedback/existing evidence? (please tick)

□ **National Reports** □ **Internal Audits**
□ **Patient Surveys** □ **Staff Surveys** □ **Complaints/Incidents**
□ **Focus Groups** □ **Stakeholder groups** √**Previous EIAs**
□ **Other**

If other please state:

Evidence	**What does it tell me? (about the existing service/policy/process? Is there anything suggest there may be challenges when designing something new?)**
National Reports	**N/A**
Patient Surveys	**N/A**
Staff Surveys	**N/A**
Complaints and Incidents	**N/A**
Results of consultations with different stakeholder groups – staff/local community groups	**N/A**
Focus Groups	**N/A**
Other evidence (please describe)	**N/A**

STEP 2 - IMPACT ASSESSMENT

What impact will the new policy/system/process have on the following: (Please refer to the 'EIA Impact Questions to Ask' document for reference)

Age A person belonging to a particular age

No impact identified

Disability A person who has a physical or mental impairment, which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities

No impact identified

Gender reassignment (including transgender) Medical term for what transgender people often call gender-confirmation surgery; surgery to bring the primary and secondary sex characteristics of a transgender person's body into alignment with his or her internal self-perception.

No impact identified

Marriage and civil partnership Marriage is defined as a union of a man and a woman (or, in some jurisdictions, two people of the same sex) as partners in a relationship. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'. Civil partners must be treated the same as married couples on a wide range of legal matters

No impact identified

Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context.
No impact identified
Race It refers to a group of people defined by their race, colour, and nationality, ethnic or national origins, including travelling communities.
No impact identified
Religion or belief Religion is defined as a particular system of faith and worship but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.
No impact identified
Sex/Gender A man or a woman.
No impact identified
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes
No impact identified
Carers A family member or paid helper who regularly looks after a child or a sick, elderly, or disabled person
No impact identified
Other identified groups such as deprived socio-economic groups, substance/alcohol abuse and sex workers
No impact identified

STEP 3 - ENGAGEMENT **AND INVOLVEMENT**

How have you engaged stakeholders in testing the policy or process proposals including the impact on protected characteristics?
No engagement undertaken as this policy has received minor amendments only
Please list the stakeholders engaged:

STEP 4 - METHODS OF COMMUNICATION

What methods of communication do you plan to use to inform service users of the policy?
□ **Verbal – stakeholder groups/meetings** □ **Verbal - Telephone** □ **Written – Letter** □ **Written – Leaflets/guidance booklets** □ **Email** √ **Internet** □ **Other**
If other please state:

ACCESSIBLE INFORMATION STANDARD

The Accessible Information Standard directs and defines a specific, consistent approach to identifying, recording, flagging, sharing and meeting the information and communication support needs of service users.

Tick to confirm you have you considered an agreed process for:
√ **Sending out correspondence in alternative formats.** √ **Sending out correspondence in alternative languages.** √ **Producing / obtaining information in alternative formats.** √ **Arranging / booking professional communication support.** √ **Booking / arranging longer appointments for patients / service users with communication needs.**
If any of the above have not been considered, please state the reason:

STEP 5 - SUMMARY OF POTENTIAL CHALLENGES

Having considered the potential impact on the people accessing the service, policy or process please summarise the areas have been identified as needing action to avoid discrimination.

Potential Challenge	What problems/issues may this cause?
None identified.	

STEP 6- ACTION PLAN

Ref no.	Potential Challenge/ Negative Impact	Protected Group Impacted (Age, Race etc.)	Action(s) required	Expected Outcome	Owner	Timescale/ Completion date

Ref no.	Who have you consulted with for a solution? (users, other services, etc.)	Person/ People to inform	How will you monitor and review whether the action is effective?

SIGN OFF

Completed by:	**Alan Clement, Senior Governance Officer**
Date:	**June 2018**
Presented to: (appropriate committee)	**Governance and Risk Committee**
Publication date:	**July 2018**