Trust Policy		NHS Worcestershire Acute Hospitals NHS Trust

Code of Conduct in Respect of Confidentiality

Department / Service:	Information Governance
Originator:	Information Governance Manager
Accountable Director:	Chief Digital Officer
Approved by:	Information Governance Steering Group, TME
Date of approval:	16th October 2025
Review Date: **This is the most current document and is to be used until a revised version is in place**	16th October 2028
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:

All employees and those working on behalf of the Trust are responsible for maintaining confidentiality and data security. This duty of confidentiality is written into employment contracts. Breach of confidentiality of information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal.

This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

Key amendments to this document

Date	Amendment	Approved by:
June 2017	Updated into trust format Update of Personal Identifiable Data (PID) to Personal Confidential Data PCD Added quick reference guide Removed reference to WHITS, Updated email flowchart Updated Social media (5.7) Abuse of Privilege (5.6), and Carelessness (5.8)	IG Manager
4th December 2019	Document extended for 6 months whilst review process is undertaken	
23rd December 2020	Document extended for 3 months until March 2021 due to urgent COVID	Rebecca Brown
31st March 2021	Document extended for 6 months as per Trust agreement 11.02.2021	
14th October 2021	Document extended for 6 months to allow updates	
3rd March 2022	Document extended to the end of June to allow for thorough review	IG Manager and Deputy SIRO
12th April 2022	Document extended to the end of September to allow for thorough review	IG Manager and Deputy SIRO
October 2022	Complete review and update	IGSG/TME
October 2025	Review and minor updates	IGSG

Contents page:

Appendices

Supporting Documents

Supporting Document 1	Equality Impact Assessment
Supporting Document 2	Financial Risk Assessment

Quick Reference Guide

Quick Reference Guide: Code of Conduct in Respect of Confidentiality

All employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 2018, General Data Protection Regulation (GDPR), the NHS Code of Practice on Confidential Information 2014, any other appropriate professional codes of conduct and the Caldicott Principles

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment. Any breaches of this code could lead to disciplinary action or dismissal.

The Trust is legally required to report and serious incidents/breaches to the police and the Information Commissioners Office and can result in prosecution and fines

To understand your responsibilities and protect patient and staff personal identifiable information (PII) ensure you complete your mandatory annual Data Security Awareness Training. It is vital that all staff, undertake annual training

PII is health related data that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Complete your mandatory annual Data Security Awareness Training

Keep passwords secure and never share your password

Lock your PC screen when the PC is not in use

Make sure that any computer screens, or other displays of information, cannot be seen by the general public.

If emailing PII use nhsmail to nhsmail. If either end not nhsmail then the email must be encrypted

Manager to ensure contractors sign contractor's confidentiality form

Do not leave any medical records or confidential information, including diaries, lying around unattended

Ensure you cannot be overheard when discussing personal/confidential information in public places/work areas

Do not include any identifiable information when using instant messaging or social media groups

All documents within patients records must be secured, with no loose paperwork

Record information accurately, in the right place and at the correct time

Always check letters are sent to the correct patient at the correct address and not containing other patients information

Ensure the correct paperwork is provided to patients such as discharge summaries

It is strictly forbidden to view or discuss any information relating to your own records, or the records of your family, staff or acquaintances unless you are directly involved in their care

Remember it is your responsibility to keep any paperwork which contains patient or staff PII secure at all times and disposed of in confidential waste.

Handover Sheets: nurses must not remove from the wards and medical staff are personally responsible for keeping information secure at all times

1. Introduction

All employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 2018, General Data Protection Regulation (GDPR), the NHS Code of Practice on Confidential Information 2014 and any other appropriate professional Codes of Conduct. Click on this link to see the Data Protection Guidance Pages

This means that employees are obliged to keep any personal confidential data strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business in confidence information such as waiting list data, consultant's workloads, business meeting minutes and financial details.

Disclosure and sharing of Personal Confidential Data is governed by the requirements of Acts of Parliament and Common Law of Confidentiality. There are exceptions where it is sufficiently in the public interest to warrant a breach of disclosure, for example in relation to a serious crime or in instances to prevent serious harm or abuse. In these circumstances staff should refer to the Trust's Freedom to Speak Up (Raising Concerns) Policy.

This Code of Conduct for Employees in Respect of Confidentiality does not override the Trust's Freedom to Speak Up (Raising Concerns) Policy.

The principle behind this Code of Conduct (Code) is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.

This Code has been written to meet the requirements of:

- The Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988

Both organisations and individuals can be held accountable for breaches of the Data Protection Act 2018. Breaches can result internally in disciplinary action and in serious cases dismissal. Externally the Information Commissioners Office (ICO) can prosecute and fine both organisations and individuals. (Click on this link to see examples of ICO notices)

The Trust carries out spot check audits and monitoring to ensure staff are following confidentiality guidance and complying with the contents of this policy and examples of non-compliance will be reported to line managers.

The audit checks will be reported to the Information Governance Steering Group.

Transfer of Personal/Confidential Data & Bulk Data

Personal data can relate to information held about any individual, not just patients and may relate to information about staff, contractors, visitors and members of the public

Information which can identify an individual includes:

- Patient's name.
- Patient's Address.
- Full post code.
- Date of birth.
- Pictures, photographs, videos, audiotapes or other images of patients.
- NHS number and local patient identifiable codes.
- Any grouping term such as 'baby', 'new-born baby'.
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

Bulk data is defined informally as person identifiable data relating to 51 or more individuals.

It should be noted the loss of a lower number of highly sensitive records is likely to have a greater impact than the loss of greater number of less sensitive records.

Any loss of data must be reported to the Information Governance and on DATIX, the Trusts incident reporting system, as soon as the loss has been discovered.

2. Scope of this document

This policy applies to all employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students.

Employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment.

3. Definitions

IGSG	Information Governance Steering Group
PII	Personal Identifiable Information
DSPT	Data Security and Protection Toolkit
DATIX	Trusts incident reporting system
SIRO	Senior Information Risk Officer
SIAO	Senior Information Asset Owner
IAO	Information Asset Owner
IAA	Information Asset Assistant
ICO	Information Commissioners Office
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service-user information

4. Responsibility and Duties

4.1 Management Responsibility

The Information Governance Steering Group is responsible for approving and implementing this policy. Managers are responsible for briefing staff regarding the contents of the policy, investigating incidents and ensuring staff complete their annual Data Security Awareness training.

Managers are responsible for ensuring contractors have signed the WAHT- Third Party Access and Non-Disclosure Agreement before they commence work at the Trust.

Managers are responsible for ensuring staff are informed regarding any personal information that is shared about them with any external agencies

4.2 Staff Responsibilities

This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. All staff has a duty to understand and comply with this Code of Conduct.

Any breach of these requirements must be reported as an incident in line with the Trust's Incident Reporting Policy and investigated to an appropriate level.

All confidential breaches reported at the Information Governance Steering Group. The Information Governance Manager will follow up actions from the Steering Group and send out relevant staff guidance in order to reduce the risk of further incidents.

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment. Any breaches of this code could lead to disciplinary action or dismissal.

Staff must be aware that the ICO can fine organisations up to £17million or 4% of global turnover for serious data breaches. Individuals can be prosecuted for breaches of personal data (including inappropriate access, sharing or loss of personal information) facing court appearances and financial penalties.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Therefore, all staff must complete their mandatory annual Data Security Awareness training to ensure they are aware of their responsibilities in relation to handling data.

4.3 Senior Information Asset Owners (SIAO)/Information Asset Owners (IAO) responsibilities

In line with the requirements of the Data Security and Protection Toolkit, the divisional directors within the Trust are SIAO's. Their primary responsibility is to manage and report any information risks within their area to the Senior Information Risk Owners.

SIAO's are supported in their role by IAO's and these staff are likely to be heads of departments or system administrators.

5. Code of Conduct in Respect or Confidentiality Policy Detail

5.1 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

For example, information may be held on paper, disc, CD, memory stick, e-mail, computer file or printout, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops, tablets, mobile phones, memory sticks and digital cameras or other digital devices.

It can take many forms including medical notes, audits, employee records, etc. It also includes any Trust business confidential information.

Personal Identifiable Information (PII) is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. health data)

During your work duties you should consider all information to be sensitive, even something such as a patient's name and address. The same standards should be applied to all information you come into contact with.

National Opt-out
Everyone has the right to opt-out of their health data being used for the purposes of research and planning. NB The opt-out does not apply to sharing data for direct patient care. This is a national programme and patients can opt out either online or through a telephone service. Click here for a link to 'your-nhs-data-matters'

5.2 Requests for Information regarding Patients/Staff

- Staff should not give out information on patients or staff to unauthorised persons who do not "need to know" in order to provide health care, treatment or regarding employment.
- All requests for identifiable information should be based on a justified need and some may also need to be agreed by the Trust's Confidentiality Lead (Caldicott Guardian).

Any exceptions to this rule may require you to get written consent from the patient or staff member in advance.

If the patient is unconscious and unable to give consent, consult with the health professional in charge of the patient's care. Click Here for link to GMC Capacity Issues webpage.

Whether you are requesting, using or disclosing PII or confidential information you should at all times abide by the Caldicott Principles. These are:

- **Principle 1: Justify the purpose(s) for using confidential information**
  Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.
- **Principle 2: Use confidential information only when it is necessary**
  Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

- **Principle 3: Use the minimum necessary confidential information**
  Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.to
- **Principle 4: Access to confidential information should be on a strict need know basis**
  Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.
- **Principle 5: Everyone with access to confidential information should be aware of their responsibilities**
  Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.
- **Principle 6: Comply with the law**
  Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out the common law. in statute and under
- **Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality**
  Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employ ers, regulators and professional bodies.
- **Principle 8: Inform patients and service users about how their confidential information is used**
  A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information required. Published December 2020 in some cases, greater engagement will be

If you have any concerns about disclosing/sharing patient/staff information you must discuss this with your manager and if they are not available, someone with the same or similar responsibilities. Alternatively, if you are uncertain whether disclosure of information can take place please email the Trust's Confidentiality Lead (Caldicott Guardian)

5.3 Requests for Patient Information by:

5.3.1 Police, Solicitors and other law enforcement agencies who may have regulatory powers to request information
Contact legal services via switchboard

All out of hours Police requests should be directed to the on-call manager

5.3.2 Local Authority Designated Officer (LADO) for safeguarding issues:
Contact the Safeguarding Team within the Trust on wah-tr.safeguardingworcsacute@nhs.net

5.3.3 Media (unless written permission has been obtained from the patient)

- Do not give out any information under any circumstances.
- Only Directors/Senior Managers and/or the Communications Department are authorised to do so. If you receive any request from the media by personal visit or by phone refer the person to the Communications Department on wah-tr.communications@nhs.net

5.4 Requests for Staff Information by:

5.4.1 Police, Solicitors and other law enforcement agencies who may have regulatory powers to request information
Contact legal services via switchboard

All out of hours Police requests should be directed to the on-call manager

5.4.2 Media (unless written permission has been obtained from the patient)

- Do not give out any information under any circumstances.
- Only Directors/Senior Managers and/or the Communications Department are authorised to do so. If you receive any request from the media by personal visit or by phone refer the person to the Communications Department on wah-tr.communications@nhs.net

This policy does not take away the rights of a member of staff to discuss their personal employment position with their appointed solicitor or union representative

5.5 Disclosure of Information to Other Employees of the Trust

Information on patients/staff should only be released on a need-to-know basis.

- Always check the member of staff is who they say they are by asking to see their Trust ID badge
- Always check that the requestor has a legitimate right to access the information
- If a request is for patient information, check with the consultant/doctor in charge of the patient's care
- If request is for staff information, check with your line manager or HR department
- Don't be coerced into giving out information without valid reasons.

5.6 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own records and their family, friends or acquaintances unless required for the patient's clinical care or with the employee's administration on behalf of the Trust. This includes information held in electronic and paper formats. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

There is a clear process via the Trusts Access to Health Records procedure, where staff can obtain copies of their own clinical records and Subject Access Requests Policy to deal with requests for employment records.

Staff must only access/view information which is directly related to the work they are undertaking. Even if there is a legitimate reason for access if any member of staff subsequently discusses patient or staff information with other members of staff who are not directly involved in the care or with their family or friends this will be treated as a breach of confidentiality.

To protect yourself as a member of staff, it is good practice to ask a colleague to handle any information of a friend/relative/colleague.

Inappropriate access would be where you accessed PII for patients or staff where you are **not** directly involved with their care/management OR you have **not** been tasked to carry out an audit / research or investigation. This is not only a breach of Trust policy, but a breach of the Data Protection Act 2018, where you could be liable for prosecution.

If you have concerns about this issue please discuss with your line manager.

5.7 Maintaining confidentiality while working remotely

While working remotely, staff are personally responsible for maintaining the security and confidentiality of all records by:

- Adhering to a clear desk policy.
- Locking devices when unattended or when non-trust individuals are present
- Ensuring that personal identifiable information is not visible to family members, friends, or colleagues at any time.
- Preventing confidential conversations from being overheard.

5.8 Process/Projects that may the impact confidentiality of data

Prior to any new systems or changes in processes which affects the processing of PII, a Data Protection Impact Assessment (DPIA) – click this link to go to the Data Protection by Design webpage. At this point any new flows of PII will be recorded and an assessment will be carried out to establish if a Data Sharing/Processing Agreement (DSPA) is required.

5.9 Staff Representatives

This Policy will not take away the right and responsibility of a Staff Representative to:

- Discuss or form part of a case either within the Trust or with solicitors or speak and discuss with any outside bodies with whoever is deemed necessary in pursuit of their trade union duties always recognising that the confidentiality of individuals must be maintained at all times.

5.10 Interpretation

If any person requires an explanation concerning the interpretation or the relevance of this Code of Conduct in Respect of Confidentiality, they should discuss the matter with their line manager or the Trust's Confidentiality Lead (Caldicott Guardian).

5.11 Non-Compliance

Non-compliance with this code of conduct by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary policy and may lead, in very serious cases, internally to dismissal for gross misconduct, and external reporting to the police or the ICO

To obtain a copy of the disciplinary policy, procedure and guidance, please discuss with your manager or available on the Trusts Policy pages

6. Implementation

6.1 Plan for implementation

The Information Governance Manager will ensure that this policy is available to all Divisional Managers within the Trust. It is then their responsibility to ensure that all staff groups within their area are directed to this policy.

Mandatory Data Security Awareness training covers the confidentiality of information and this is promoted within the trust on a regular basis.

6.2 Dissemination

This policy will be available on the Trust Intranet and a publication in the Trust Weekly Brief to inform staff of the update to the policy.

6.3 Training and awareness

All staff are mandated to complete Data Security Awareness training on an annual basis

7. Monitoring and compliance

Please see the monitoring table on the next page for monitoring and compliance details

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the Policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Section 4.2	Any breach of these requirements must be reported as an incident in line with the Trust's Incident Reporting Policy and investigated to an appropriate level.	Regular monitoring of confidentiality breaches on DATIX	Daily	IG manager	Information Governance Steering Group	5 times a year
Section 4.2	Compliance with Mandatory Annual Data Security Awareness Training	Monthly training dashboard	Monthly	IG manager	Information Governance Steering Group	5 times a year

8. Policy Review

This policy will be updated every two years by the Information Governance Manager and approved by the Information Governance Steering Group to reflect the Trust's development of policies and procedures and the changing needs of the NHS or when necessary following changes to the law.

9. References

References: Code:

The Data Protection Act 2018 (DPA18)	National
EU General Data Protection Regulations 2016 (now UK GDPR and included within DPA18)	National
Freedom of Information Act 2000	National
The Human Rights Act 1998	National
The Computer Misuse Act 1990	National
Caldicott Principals	National
NHS Data Security and Protection Toolkit	National
Data Protection Good Practice – Information Commissioners Office	National
WAHT Corporate Records Management Policy	CG-127
WAHT ICT Policy	TWI-007
WAHT Information Governance Policy	CG-579
WAHT Data Protection Policy	IG-004

10. Background

10.1 Equality requirements

No impact from the equality assessment (Supporting Document 1)

10.2 Financial risk assessment

No impact from the financial risk assessment (Supporting Document 2)

10.3 Consultation

The policy has been created by the Information Governance Manager with input from the Information Governance Steering Group. The original policy has also been reviewed by the Policy Working Group.

Contribution List

This key document has been circulated to the following individuals for consultation;

Designation
Members of the Information Governance Steering Group, who include: SIRO, DPO, Caldicott Guardians, SIAO

This key document has been circulated to the following individuals for consultation;

Committee
Information Governance Steering Group

10.4 Approval Process

This policy will be approved at the Information Governance Steering Group and sent on the Joint Negotiating and Consultation Committee (JNCC) for information.

10.5 Version Control

This section should contain a list of key amendments made to this document each time it is reviewed.

Date	Amendment	By:
May 2011	Updated into Trust policy format and change to accountable director – from Director of HR to Director of Finance (SIRO)	Information Governance Manager
Sept 2012	Inclusion of social networking section and updated Confidentially Agreement	Information Governance Manager
June 2013	Incorporated any minor national requirements and updated into new policy template. Updated social media section to reflect current guidance	Information Governance Manager
April 2014	Updated following requests from Human Resources for additional guidance including passwords and secure emailing	Information Governance Manager
April 2015	Updated to include Clear Desk	IG Manager
June 2017	Updated into trust format Update of PID to PCD Added quick reference guide Removed reference to WHITS, Updated email flowchart Updated social media (5.7) Abuse of Privilege (5.6), and Carelessness (5.8)	Information Governance Manager
4th December 2019	Document extended for 6 months whilst review process is undertaken	Deputy SIRO
23rd Dec 2020	Document extended for 3 months until March 2021 due to urgent COVID work	Deputy SIRO
31st March 2021	Document extended for 6 months as per Trust agreement 11.02.2021	Deputy SIRO
14th October 2021	Document extended for 6 months to allow updates before going to JNCC	Deputy SIRO
3rd March 2022-	Document extended to the end of June to allow for thorough review	Deputy SIRO
12th April 2022	Document extended to the end of September to allow for thorough review	Deputy SIRO
October 2025	Minor updates	Head of Digital Governance

Supporting Document 1 – Equality Impact Assessment form

Equality and Health Inequalities Impact Assessment (EHIA) Tool

Herefordshire & Worcestershire STP - Equality and Health Inequalities Impact Assessment (HEIA) Form
Please read HEIA guidelines when completing this form

Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust	x	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

Name of Lead for Activity	

Details of individuals completing this assessment	**Name**	**Job title**	**e-mail contact**
	Matthew Thurland	**Head of Digital Governance and Compliance**	**Wah-tr.dataprotection@nhs.net**
Date assessment completed			

Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	**Title: Code of Conduct in Respect of Confidentiality**			
What is the aim, purpose and/or intended outcomes of this Activity?	**Policy document to inform all staff**			
Who will be affected by the development & implementation of this activity?	❑	Service User	x	Staff
	❑	Patient	❑	Communities
	❑	Carers	❑	Other _____
	❑	Visitors	❑	
Is this:	x Review of an existing activity ❑ New activity ❑ Planning to withdraw or reduce a service, activity or presence?			

What information and evidence have you reviewed to help inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.	Reviewed in line with national guidance
Summary of engagement or consultation undertaken (e.g. who and how have you engaged with, or why do you believe this is not required)	WAHT Information Governance Steering Group
Summary of relevant findings	Approved

Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group and explain your rationale**. Please note it is possible for the potential impact to be both positive and negative within the same equality group and this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	Potential positive impact	Potential neutral impact	Potential negative impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Age		X		
Disability		X		
Gender Reassignment		X		
Marriage & Civil Partnerships		X		
Pregnancy & Maternity		X		
Race including Traveling Communities		X		
Religion & Belief		X		
Sex		X		
Sexual Orientation		X		
Other Vulnerable and		X		

Equality Group	Potential positive impact	Potential neutral impact	Potential negative impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)				
Health Inequalities (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		X		

Section 4

What actions will you take to mitigate any potential negative impacts?	Risk identified	Actions required to reduce / eliminate negative impact	Who will lead on the action?	Timeframe
		.		
How will you monitor these actions?				
When will you review this EIA? (e.g in a service redesign, this EIA should be revisited regularly throughout the design & implementation)				

Section 5 - Please read and agree to the following Equality Statement

1. Equality Statement

1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on the 9 protected characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation

1.2. Our Organisations will challenge discrimination, promote equality, respect human rights, and aims to design and implement services, policies and measures that meet the diverse needs of our service, and population, ensuring that none are placed at a disadvantage over others.

1.3. All staff are expected to deliver services and provide services and care in a manner which respects the individuality of service users, patients, carer's etc, and as such treat them and members of the workforce respectfully, paying due regard to the 9 protected characteristics.

Signature of person completing EIA	
Date signed	
Comments:	
Signature of person the Leader Person for this activity	
Date signed	
Comments:	

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval