CONFIDENTIALITY AUDIT POLICY

			POLICY
Reference	IG/003		
Approving Body	Information Governance Committee		
Date Approved	JULY 2025		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	31 JULY 2025		
Version	6		
Summary of Changes from Previous Version	Fact-find procedure		
Supersedes	5		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Committee Information Governance Working Group		
Date of Completion of Equality Impact Assessment	12th January 2023 Updated 14th May 2025		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	UK General Data Protection Regulation Data Protection Act 2018 Human Rights Act 1998 Common law duty of confidentiality Regulation of Investigatory Powers Act 2000 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 The Network and Information Systems Regulations 2018 Computer Misuse Act 1990		
Target audience	All staff		
Review Date	July 2027		
Sponsor (Position)	Chief Digital Information Officer		
Author (Position & Name)	Jacquie Widdowson, Head of Data Security & Privacy /Data Protection Officer		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Head of Data Security and Privacy		
Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**		
Information Security Policy	JULY 2025		
Template control	April 2024		

CONTENTS

APPENDICIES

1.0 INTRODUCTION

The National Health Service (NHS) Care Record Guarantee[1] and Confidentiality NHS Code of Practice[2] requires that all NHS organisations put in place mechanisms in place to handle sensitive or personal confidential data. This requires access to confidential information to be monitored and audited locally and requires that there are agreed procedures for investigating confidentiality alerts.

Sherwood Forest Hospitals NHS Foundation Trust is required to have processes in place to highlight actual or potential confidentiality breaches in its systems, in particular where sensitive information or personal confidential data is held. The Trust is also required to have procedures in place to evaluate the effectiveness of controls within these systems. All systems which process sensitive or personal data should have audit trails that can report who has viewed, accessed, altered or deleted data.

The Human Rights Act 1998, Article 8 relates to the right of Privacy. If information is inappropriately disclosed the individual can take legal action for breach against the public body concerned. Not only must patient information be held confidentially, but it must also be held securely. Failure to do so will also breach the right to respect for private life

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purpose may result in a breach of confidentiality, thereby contravening Data Protection legislation, the Human Rights Act 1998 and the common law duty of confidentiality.

2.0 POLICY STATEMENT

The Trust has a responsibility to maintain the confidentiality, integrity and availability of information held both manually and electronically. This document defines the procedure for carrying out audits and monitoring relating to access to person identifiable data (PID) and personal confidential data (PCD).

This document sets out the appropriate confidentiality audit procedure to monitor access to confidential patient/employee information. This includes:

- How access to confidential information will be monitored
- Who will carry out the monitoring/auditing of access
- Reporting and escalation processes
- Disciplinary processes.

[1] https://www.cht.nhs.uk/fileadmin/site_setup/contentUploads/Patient_Vistors/Your_health_record/NHS_Care_Record_Guarantee.pdf

[2] https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

The procedure also ensures that overall responsibility for monitoring and auditing access has been assigned to appropriate senior staff members, e.g. Senior Information Risk Officer (SIRO) and Caldicott Guardian, Head of Data Security & Privacy/Data Protection Officer or Information Asset Owner (IAO). Confidentiality audits will focus primarily on controls within electronic records management systems but should not exclude paper records. The purpose being to discover instances of inappropriate access and whether confidentiality has been breached or put at risk through deliberate misuse of access or because of weak, or non-existent or poorly applied controls.

This document defines the procedure for carrying out audits relating to inappropriate access to confidential patient/employee information within the Trust. The Trust must ensure that confidential patient/employee information is only accessible to staff who have a legitimate relationship or where there is a legitimate business need, inline with the DSPT[3], NHS care record guarantee[4] and compliance with data protection legislation[5].

With advances in the electronic management of information within the NHS, the requirement to monitor access to personal confidential information has become increasingly important. Furthermore, with the increased movement of information via electronic communications, there exists an increasing threat of information being accessed by individuals who do not have a legitimate relationship and a legal right to access it.

3.0 DEFINITIONS/ ABBREVIATIONS

CQC	Care Quality Commission
DoH	Department of Health & Social Care
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
DSPT	Data Security and Protection Toolkit
NCRS	NHS Care Record Guarantee
SIRO	Senior Information Risk Owner
PID	Personal Identifiable Data
PCD	Personal Confidential Data

[3] https://www.dsptoolkit.nhs.uk/

[4] https://www.cht.nhs.uk/fileadmin/site_setup/contentUploads/Patient_Vistors/Your_health_record/NHS_Care_Record_Guarantee.pdf

[5] https://www.gov.uk/data-protection

DPO	Data Protection Officer

4.0 ROLES AND RESPONSIBILITIES

Caldicott Guardian

It is a requirement for all NHS organisations to appoint a Caldicott Guardian, who must be a senior person within the organisation. The Chief Medical Officer is the Trust's appointed Caldicott Guardian and has overall responsibility for protecting the confidentiality of people's health and care information and making sure that it is used appropriately. The SIRO and Caldicott Guardian will be informed where serious breaches occur, they will also be updated with the findings of any confidentiality audits and ensure that appropriate action is taken.

The Caldicott Guardian will also be responsible for ensuring that access to personal confidential information remains relevant and is regularly audited within the Trust and will be responsible for monitoring incidents and complaints relating to confidentiality breaches within the Trust and work closely with the Head of Data Security and Privacy/ DPO.

SIRO

The SIRO is responsible for managing information risks within public organisations. The SIRO ensures awareness of information risk responsibilities, safeguards information appropriately and advises the board on risk mitigation.

Will be updated via a report to the Information Governance Committee or by the Head of Data Security & Privacy on all inappropriate access to systems and system security breaches.

Head of Data Security & Privacy

The Head of Data Security/ DPO will be responsible for ensuring that access to PID and PCD is audited and monitored within the Trust. Ensuring that reports from the clinical systems and other local systems are reviewed and followed-up and provide reports to the Information Governance Committee.

Information Governance Department

The role of the Head of Data Security & Privacy/Data Protection Officer is to help ensure the Trust's handling and sharing of personal data is undertaken in a confidential and secure manner, to appropriate ethical, professional and legal standards.

They will provide advice or participate in the investigations of breaches of confidentiality as required.

The Information Governance Committee

The Information Governance Committee will be responsible for ensuring that audit and monitoring procedures are implemented throughout the Trust in line with requirements.

People Directorate

Will be informed where serious breaches occur, requesting confidentiality audits where applicable supporting leaders to manage staff where breaches occur via Human Resources Policies and Procedures.

Information Asset Owners / System administrators

Information Asset Owners (IAOs) are responsible for ensuring that access to confidential patient/employee information is secure and strictly controlled within their Divisions/Departments.

Information Asset owners will ensure that staff they are responsible for are aware of their responsibility regarding confidentiality of information. They will be responsible for complying with auditing and monitoring and ensuring that subsequent recommendations are complied with, within specified timescales.

Monitoring of clinical systems should be carried out by the responsible administrator/manager, such that instances of alleged inappropriate access or misuse of confidential information can be identified and reported to the IG department for action to be taken. Support on how and when to conduct a confidentiality audit will be provided by the IG department.

Access to confidential patient/employee information must be allocated on a strict need to know basis, by those who require such access to perform their duties. Appropriate documented authorisation must be obtained to demonstrate the need to know prior to additional access being given.

Requests to audit a user will only be provided to IT Services (Nottinghamshire Health Informatics Service – NHIS) and System Administrators once the request has been authorised and sanctioned by both the Information Governance department and the Operational People Directorate Team.

All Staff

Staff may also report concerns relating to potential breaches of confidentiality, which may result in an audit of user access and activity on the relevant Trust system(s).

All investigations and outcomes will be recorded by the IG department and passed on to the operational People Directorate for further action, which may include an initial fact-finding

meeting, and potentially disciplinary investigation and action against the member(s) of staff involved, the implementation of additional controls, or other remedial action as necessary.

Actual or potential breaches of inappropriate access should be reported to the IG department immediately and an incident report completed on the Trusts incident reporting system (Datix).

All staff, whether permanent, temporary or contracted, should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality.

5.0 APPROVAL

The Confidentiality Audit Policy will be approved at the Trust's IG Committee.

6. MONITORING AND AUDITING ACCESS TO CONFIDENTIAL INFORMATION

All work areas within the Trust which processes confidential information will be subject to a confidentiality audit.

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis. This will be achieved by putting in place arrangements for both proactive and reactive auditing of access to confidential information and communicated to all staff.

Proactive Monitoring

This will generally be achieved for systems where an automated function exists for the alerting of user access to records for subsequent review by someone with Caldicott Guardian, SIRO, IAO or Information Governance roles within the system.

Examples of proactive monitoring on systems accessed by Trust staff include;

- SystmOne
- Orion.

Automatic system alerts are generated when staff override any of the privacy controls that are in place.

These alerts will prompt the receiving staff member to establish if the access was justified or potentially inappropriate, which will warrant further investigation. A proportionate sample size of alerts will need to be reviewed on a monthly basis.

Privacy monitoring tools will also be used for proactive monitoring of staff access to records and systems. The monitoring tool will examine staff access to identify any suspicious or potentially

inappropriate patterns for further investigation by the Information Governance department. The outcome of these reviews will be escalated to People Directorate for further investigation as appropriate.

Reactive Monitoring

Reactive confidentiality audits will generally fall into 2 scenarios:

System access misuse reported regarding data breaches, including inappropriate access and confidentiality issues.

Evidence is necessary to support line manager inquiries about staff behaviour, such as excessive internet usage, email activity, or conduct. These concerns are not primarily focused on breaches of privacy or confidentiality, though audit information may have privacy implications. Line manager inquiries will also be governed by relevant policies, including the Information Security Policy and the Email and Internet Policy.

Auditing Process

The Head of Data Security & Privacy/ DPO will request that a report be generated for a random sample of 20 patients at least twice annually. This report will be produced by system administrators or the Information Governance Team. It will cover the period of the previous month from the date of the request. Each report will then be shared with the pertinent Information Asset Owner of the employee identified in the audit to ascertain the legitimacy and appropriateness of the access. The findings from these internal investigations will be communicated to the Head of Data Security & Privacy/ (DPO) for inclusion in the report.

If concerns arise from the report's outcome, the Head of Data Security and Privacy/DPO will forward the report to the People Directorate for handling in accordance with the Trust's disciplinary procedures. The SIRO and Caldicott Guardian will be notified immediately.

The audit process will be carried out at least twice yearly.

- The information contained within the audit will consist of the following information:
- Unauthorised viewing or access to confidential patient or staff records
- Repeated attempts of accessing confidential information
- If appropriate access is identified, then a further audit will be run to identify of any changes to information have been made.
- Evidence of shared login or passwords

- Inappropriate communications with patients or staff
- Inappropriate recording and or use of sensitive patient or staff information
- Inappropriate allocation of access rights to the system or data
- Inappropriate staff access to the secure or restricted physical areas
- Reports and findings from the audit will be presented to the Information Governance Committee

Monitoring Process

In order to provide assurance that access to PID or PCD is gained only by those individuals that have a legitimate right of access, it is necessary to ensure that appropriate monitoring is undertaken either when a concern regarding inappropriate access is identified or by the means of periodic audits or monitoring is undertaken.

The information asset owner is responsible for assisting with audits to identify and report irregularities in accessing confidential information to the information governance department. Appropriate action will then be taken, which may include disciplinary measures, the implementation of additional controls, or other necessary remedial actions.

Actual or potential breaches of confidentiality should be reported to the information governance team or people directorate immediately, in order that action can be taken to prevent further breaches taking place. This also gives the Head of Data Security & Privacy/DPO the opportunity to assess if the incident falls into the threshold of the serious incident category and reportable to the ICO (Information Commissioner Office). The Head of Data Security/DPO will be responsible for ensuring that the Information Governance Committee are informed of any concerns.

Requests for Audits or Monitoring or access to personal data

- Request for audit or monitoring or access to personal data to be submitted to information governance or people directorate.
- Form authorised by Director of People or Deputy Director of People
- People Directorate forward form onto Head of Data Security/ DPO who will provide confirmation of approval to proceed with audit or request further information.
- Requests for audits to be undertaken via the IG Team or appropriate IAO/System Administrators

- Results returned to information governance team and relevant information forwarded to People Directorate.

7.0 CONFIDENTIALITY AUDIT AND ESCALATION PROCESS

The response to an IG breach will be considered on an individual basis.

Where an audit of user activity or access to records is required as part of a fact-find, the request should be initiated by the line manager or an appropriate senior manager. The People Directorate may also request audits. Audit requests must include a brief outline of the report/allegation and information required, giving justification of the relevance of the audit information to the investigation.

The form located in Appendix A must be completed for all audit requests and forwarded to the IG team sfh-tr.information.governance@nhs.net or directly to the Head of Data Security & Privacy. The IG team will ensure that a legitimate and lawful reason for access to the information is provided. Consent will be obtained if appropriate. Caldicott Principles must be adhered to at all times, with only the relevant and minimum information being shared regarding the need for the audit.

Approved requests will be sent to appropriate system administrators in the Trust for processing.

Upon completion of the audit, system administrators will provide the audit report to the IG team to review and remove any irrelevant information and feed back to the People Directorate. It is important that audit reports are only seen by as few staff as possible; likewise, the audit report must be kept secure.

Investigation audits may identify evidence of:

- Unauthorised viewing/access to confidential/patient/staff records
- Failed attempts to access confidential information
- Repeated attempts to access confidential information
- Successful access of confidential information by unauthorised staff
- Evidence of shared login sessions/passwords and smartcards
- Inappropriate communications with patients
- Inappropriate recording and/or use of sensitive/patient information
- Inappropriate allocation of access rights to systems or other data
- Inappropriate staff access to secure/restricted physical areas.

Investigating Confidentiality Events and Alerts

The Information Governance team, where required, will be responsible for liaising with the People Directorate to co-ordinate investigations into confidentiality breaches.

Investigation and management of confidentiality events and alerts will be in line with the Trust's Disciplinary Policy[6] and Data Protection, Confidentiality and Disclosure Policy[7].

Inappropriate Access to Systems

Staff who have inappropriately accessed a record will receive a 'soft' or 'hard' letter, depending on the individual situation, reinforcing the requirement to adhere to Information Governance policies and procedures[8] at all times. The letter advises that a further repeat of this could result in a Fact Finding exercise or formal Disciplinary action.

Staff who have inappropriately accessed a record and receives a 'hard' letter will be issued with an invite to meet to undertake a fact-finding exercise to ascertain the reasons behind accessing the record. On completion of the fact find, the information will be reviewed and a decision will be made regarding the next steps. One outcome of the fact find could be that it proceeds to a formal investigation under the Trust's Disciplinary policy.

Providing Audit Information To Patients/Service Users

Both the National Information Board in 'Personalised Health and Care 2020'[9] and Dame Fiona Caldicott in the 'Report of the Caldicott2 Review'[10] have reaffirmed the commitment made in the NHS Care Record Guarantee[11] to ensure that a record of who has accessed a service user's health records can be made available in a suitable form to service users on request. All requests of this nature need to be directed to the IG team

8.0 MANAGEMENT OF DATA BREACHES (IG INCIDENTS)

The IG team proactively monitor data breach incidents logged in the Trusts incident reporting system, Datix. The IG team will review, provide guidance and follow up all data breach incidents to ensure a satisfactory outcome in liaison with investigators. More serious data breach incidents are recorded on NHS Digital's Data Security and Protection Toolkit[12]. All data breaches are reported to the IG Committee, which will escalate any unsatisfactory outcomes to Audit and Risk Committee and communicate pertinent IG issues/messages to staff using, for example, Trust Briefing and intranet notice board bulletins/icare2. Trends in incidents will be monitored in order to learn lessons and provide continual service improvement.

[6] https://www.sfh-tr.nhs.uk/media/rhqnw4ps/disciplinary-policy.pdf
[7] https://www.sfh-tr.nhs.uk/media/1gelq1ev/data-protection-confidentiality-and-disclosure-policy.pdf
[8] https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/
[9] Personalised health and care 2020 - GOV.UK
[10] https://www.gov.uk/government/publications/the-information-governance-review
[11] https://www.cht.nhs.uk/fileadmin/site_setup/contentUploads/Patient_Vistors/Your_health_record/NHS_Care_Record_Guarantee.pdf
[12] https://www.dsptoolkit.nhs.uk/

9.0 RELEVANT POLICIES AND PROCEDURES[13]

- Corporate Records Policy
- Data Protection, Confidentiality and Disclosures Policy
- Data Quality Policy
- Disciplinary Policy
- Internet and Email and Internet Policy
- Freedom of Information Act Policy and Procedure
- Health Records Management Policy
- Information Governance Policy
- Information Security Policy
- Retention and Destruction Policy.

10.0 EQUALITY AND DIVERSITY STATEMENT

All patients, employees and members of the public should be treated fairly and with respect, regardless of age, disability, gender, marital status, membership or non-membership of a trade union, race, religion, domestic circumstances, sexual orientation, ethnic or national origin, social & employment status, HIV status or gender re-assignment.

All trust policies and trust wide procedures must comply with the relevant legislation (non-exhaustive list):

- Code of Practice on Age Diversity in Employment (1999)[14]
- Disability Discrimination Act (1995)[15]
- Employment Equality (Age) Regulations 2006[16]
- Employment Equality (Religion or Belief) Regulations 2003[17]
- Employment Equality (Sexual Orientation) Regulations 2003[18]
- Employment Relations Act (1999)[19]
- Equal Pay Act (1970 and amended 1983)[20]
- Equality Act (Sexual Orientation) Regulations 2007[21]
- Fixed Term Employees - Prevention of Less Favourable Treatment Regulations (2001)[22]
- Health & Safety at Work Act 1974[23]

[13] https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/
[14] https://edm.parliament.uk/early-day-motion/17570/age-diversity-in-employment-code-of-practice
[15] https://www.legislation.gov.uk/ukpga/1995/50/contents
[16] https://www.legislation.gov.uk/uksi/2006/1031/contents
[17] https://www.legislation.gov.uk/uksi/2003/1660/contents
[18] https://www.legislation.gov.uk/uksi/2003/1661/contents
[19] https://www.legislation.gov.uk/ukpga/1999/26/contents
[20] https://www.legislation.gov.uk/uksi/1983/1794/body/made
[21] https://www.legislation.gov.uk/uksi/2007/1263/contents/made
[22] https://www.legislation.gov.uk/uksi/2002/2034/contents
[23] https://www.legislation.gov.uk/ukpga/1974/37/contents

- Human Rights Act (1998)[24]
- Part Time Workers - Prevention of Less Favourable Treatment Regulations (2000)[25]
- Race Relations (Amendment) Act 2000[26]
- Rehabilitation of Offenders Act (1974)[27]
- Sex Discrimination Act (1975 amended 1986)[28]
- Trade Union and Labour Relations (Consolidation) Act 1999[29]

[24] https://www.legislation.gov.uk/ukpga/1998/42/contents
[25] https://www.legislation.gov.uk/uksi/2000/1551/contents
[26] https://www.legislation.gov.uk/ukpga/2000/34/contents
[27] https://www.legislation.gov.uk/ukpga/1974/53
[28] https://www.legislation.gov.uk/ukpga/1986/59/enacted
[29] https://www.legislation.gov.uk/ukpga/1992/52/contents

11.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Reactive monitoring of staff access	Head of Data Security & Privacy	Staff monitoring of systems /audits	Ad-hoc -	Information Governance Committee
Proactive Monitoring of staff access to systems	Head of Data Security & Privacy	Staff monitoring of systems/audits	Daily	Information Governance Committee
Auditing	Head of Data Security & Privacy	Auditing sample of 20	6 monthly	Information Governance Committee

12.0 TRAINING AND IMPLEMENTATION

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition, all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face or online[30]. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website[31].

13.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document has not been subject to an Environmental Impact Assessment.

14.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Computer Misuse Act 1990[32]
- Confidentiality: NHS Code of Practice 2003[33]
- Data Protection Act 2018[34]
- Human Rights Act 1998[35]

[30] https://sherwood-eacademy.co.uk/login/index.php
[31] https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/
[32] https://www.legislation.gov.uk/ukpga/1990/18/contents
[33] https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
[34] https://www.legislation.gov.uk/ukpga/2018/12/contents
[35] https://www.legislation.gov.uk/ukpga/1998/42/contents

- NHS Care Record Guarantee[36]
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[37]
- UK General Data Protection Regulation[38]

Related SFHFT Documents: [39]

- Corporate Records Policy
- Data Protection, Confidentiality Policy and Procedure
- Freedom of Information Act Policy
- Health Record Keeping Policy
- Health Records Management Policy
- Information Security Policy
- Retention and Destruction Policy and Procedure

15.0 KEYWORDS

Personal confidential data, data, information, availability, integrity, confidentiality.

16.0 APPENDICES

List of appendices are provided in the contents table

36 https://www.cht.nhs.uk/fileadmin/site_setup/contentUploads/Patient_Vistors/Your_health_record/NHS_Care_Record_Guarantee.pdf
37 https://www.legislation.gov.uk/uksi/2000/2699/contents/made
38 https://www.gov.uk/data-protection
39 https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: CONFIDENTIALITY AUDIT POLICY			
New or existing service/policy/procedure: EXISTING			
Date of Assessment: 15th May 2025			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion / Belief	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be	None

		available in alternative languages, upon request	
Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None
What consultation with protected characteristic groups including patient groups have you carried out • None			
What data or information did you use in support of this EqIA? • Trust guidance for completion of equality impact assessments			
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, or comments, concerns, complaints or compliments? No			
Level of impact Low Level of Impact			
Name of Responsible Person undertaking this assessment: Jacquie Widdowson, Head of Data Security & Privacy			
Signature:			
Date: 15th May 2025			

APPENDIX 2: APPROVAL FOR STAFF MONITORING – AUDIT DATA

Name & Job Title of Requester	
Incident Number	
Date of Request	
Date of incident if known	
Name & Job Title of the employee	
Date from and to	
System to be audited	Nervecentre Careflow ICE SystmOne Email Dragon CRIS Other please list
Which act is being breached	Data Protection Act 2018 Computer Misuse Act 1990
Are you the lead investigator?	
Is this part of a People Directorate investigation, fact-find?	Yes No If no please describe
Is this a breach of Health & Safety that could jeopardise other workers	Yes No
Why do you require the information and how will the information be used and for what purpose	
Is this in relation to Criminal Activity at work or gross misconduct (please indicate severity)	
What is the timescale for the data to be provided?	
Has the member of staff been informed where the audit data may have privacy implications for the individual concerned (e.g. if emails are to be searched in the absence of the employee)? If no, then explain why.	
Has access to systems to be blocked been requested	Yes No

Signature of service lead/ Deputy Director of People Directorate :

Head of Data Security & Privacy Authorise or Decline:

Signature of Head of Data Security & Privacy:

Reason for decision eg breach of data protection Act or Computer Misuse Act

Date:

Please Note: The information produced as part of this investigation monitoring may be required to be retained on the employee's file.