NHS
Cornwall and Isles of Scilly

Information governance incident management procedure

Date approved: 11 April 2025

NHS Cornwall and Isles of Scilly Integrated Care Board

Call us on 01726 627 800
Email us at ciosicb.contactus@nhs.net
Visit our website: cios.icb.nhs.uk

Part 2S, Chy Trevail,
Beacon Technology Park,
Dunmere Road,
Bodmin, PL31 2FR
Chair: John Govett
Chief executive officer: Kate Shields

Document control

Title of document: Information Governance Incident Management Procedure
Lead directorate: Corporate Governance
Lead team: Information Governance
Document type: Protocols
Subject category: Information Governance
Author(s) name: Mike Cottam – IG Consultant and Jim George - IG Officer (NHS SCW CSU
Date ratified: 11 April 2025
Ratified by: Information Governance Steering Committee
Review frequency: 3 years (standard, unless otherwise indicated)
To be reviewed by date: 11 April 2028
Target audience: All staff
Can this policy be released under FOI? Yes

Version control

Version number	Revision date	Revision by	Nature of revisions
1.0	06/02/2025	Information Governance Consultant	First draft
1.1	11/04/2025	Information Governance Steering Committee	Ratified by IGSC
2.0	24/04/2025	Terry Willows, Company Secretary	Ratified by TW

You can request any document published on our website in alternative formats. Email our engagement team for more information.

Table of Contents

Summary of Procedure 4
1. Introduction and purpose 4
2. Scope 5
3. Definitions 6
What is a personal data breach? 6
4. Roles and responsibilities 7
5. Procedure 8
6. Reporting 10
7. Training 10
8. Equality impact assessment 11
9. Monitoring effectiveness 11
10. Distribution 11
11. Freedom of information requests (foi) 11
12. Review 12
13. References and links to other documents 12
Information Governance Incident Report 13
Information governance incident scoring matrix 15
Risk grading descriptions 15
Data Subject notification and apology letter template 16
Appendix 1: Equality impact assessment 17
Aims, objectives and purpose of the policy 17
Differential impacts 17
Human rights values 19
Public Sector Value Act 2012 19
Equality impact assessment action plan 20

Summary of Procedure

This document sets out the procedure for ICB colleagues who are responsible for the reporting, managing and investigation of information governance incidents.

The aim of the document is to ensure:

- Compliance with NHSD's Guide to Notification of Data Security & Protection Incidents
- Compliance with NIS regulations
- Compliance with ICO reporting requirements
- Compliance with the Data Security & Protection Toolkit
- Requirements of Auditors are satisfied.

This document applies to all ICB colleagues, individuals contracted to the ICB and organisations carrying out the duties on the ICB's behalf.

Annexes:

- Incident Report
- IG Incident Report Log
- Scoring Matrix
- Letter of Apology

1. Introduction and purpose

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 18) which is our current data protection legislation as regulated by the Information Commissioner's Office (ICO) require all organisations to investigate and report, all incidents that may result in a breach of the Rights and Freedoms of an individual or where a system has failed in its security, causing a cyber breach. Incidents will be logged managed, investigated and reported in line with the Data Security & Protection Toolkit.

There are timescales applied to the management and reporting of data breaches - all breaches should be reported to the IG team within 24 hours of the breach being identified. The IG Team have 48 hours to undertake an initial investigation and grading of the incident. If the breach is likely to result in a high risk to the rights and freedoms of individuals it must be reported to the Information Commissioners Office (ICO) within 72 hours and the ICB must inform those individuals without undue delay.

Cornwall and the Isles of Scilly ICB (CIOS ICB) will keep a log of all IG incidents. Where the data breach is an internal breach (a data breach originating with the ICB) the reporter will be contacted by IG and be required to provide as much information as possible to take immediate mitigating action, investigate the breach and learn lessons to try to avoid similar breaches occurring.

Reported external breaches (originating from outside the ICB (i.e. NHS Trust, Local Authority, GP etc) will be logged and any themes or regular occurrence will be noted.

Where repeat incidents are noted, the ICB contract manager will be informed, so that data security and protection can be discussed at contract review meetings.

The originator of an External incident must be informed of the incident and asked to inform their own IG so the incident can be investigated and, if necessary, reported. Where an External incident is graded as serious, the ICB will require feedback from the originating organisation regarding how they have investigated the incident. Otherwise, the incident can be closed by IG once there is confirmation that the originator has been informed and asked to report to their own IG.

CIOS ICB will use the Data Security and Protection Toolkit (DSPT) Incident Reporting Tool for any notifiable breaches. This includes personal data breaches and cyber security incidents to the ICO and other appropriate agencies.

CIOS ICB recognises the importance of reporting incidents as an integral part of its risk identification and information risk management arrangements. The benefits of incident and near miss reporting include:

- Rectifying any issues as quickly as possible to limit the breach
- Identifying trends across the organisation
- Learning lessons and strengthening processes to avoid further incidents
- Pre-empting complaints
- Making sure areas of concern are acted upon
- Targeting resources more effectively
- Increasing awareness and responsiveness.

Most information incidents relate to process failure and human error. All colleagues are encouraged to understand the contribution they make to the security and governance of information, systems and networks. The ICB takes a ‘just’ approach to IG incidents and will, where required, pursue disciplinary processes.

2. Scope

This document sets out how all information incidents will be identified, reported by colleagues and managed, including Serious Incidents (SI) and those which may be considered Information Technology or cyber related rather than Information Governance related.

It is the responsibility of all colleagues to ensure that personal confidential information and commercially sensitive information remains secure and, therefore, it is important to ensure that when incidents occur any harm is minimised and lessons are learnt.

The ICB is committed to identifying, evaluating and mitigating all risks to data subjects; these include patient/service users, colleagues and contractors.

This procedure excludes incidents not relating to information or personal data breaches.

3. Definitions

Data subject	Refers to Individuals such as patients, services users, public, colleagues or anyone impacted by an incident
DPO	Data Protection Officer
DSPT	Data Security & Protection Toolkit
ICO	Information Commissioners Office
GDPR	UK General Data Protection Regulations 2016
Notifiable incident	Notifiable breaches are those that are likely to result in a high risk to the rights of freedoms of the individual (data subject). The scoring matrix used in the reporting tool has been designed to identify those breaches that meet the threshold for notification
Personal confidential data	Refers to information that can be used to directly or indirectly identify a living individual by reference to: A personal identifier such as: a name, address, DOB, NHS No., an identification number, location data or an online identifier such as IP address. It could also contain protected identifiers such as, sexuality, religious belief, race, gender, Political choice, union membership
Special Category data	Health data including diagnosis, medication, care planning, specific protected illnesses, safeguarding
NIS Regulations	The Network and Information Systems Regulations is a requirement to report events where IT security systems have been breached causing a cyber security risk, that may have a significant impact on the continuity of essential services within 72 hours.
Internal data breach	Information breached by the ICB, for example by sharing information to an incorrect recipient; losing control of data held; unauthorised access to systems.
External data breach	Information breached by an organisation external to the ICB, where the breach is identified by the ICB or impacts on the ICB.

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Near misses should also be considered. Personal data breaches can also be called:

- Information Governance breach
- Data breach
- IG Incident
- Breach of confidentiality
- Serious Incident (SI)
- Information Security Incident

Data breaches fall into three categories:

Type of Breach	Summary	Examples (not exhaustive)
Confidentiality Breach	Unauthorised or accidental disclosure of, or access to personal data	• Personal data sent by email to incorrect recipient • Personal data posted to incorrect recipient • Personal data shared inappropriately on MS Teams/Sharepoint • Personal data included on or with an invoice • Failure to redact personal data • Personal data uploaded to website • Verbal disclosure of personal information • Failure to use "BCC" when sending emails • Cyber incident (phishing, hacking, default password not changed etc.) • Unauthorised use of Artificial Intelligence. •
Availability breach-	Unauthorised or accidental loss of access to, or destruction of, personal data	• Loss or theft of paperwork • Loss or theft of unencrypted device • Loss or theft of only copy of encrypted data • Data left in unsecure location • Insecure disposal of personal data • Insecure disposal of hardware • Personal data filed in another patient's record • Cyber incident (DDOS - distributed denial of service attack, exfiltration, weak encryption etc.)
Integrity breach	Unauthorised or accidental alteration of personal data	• Personal data entered into wrong patient record • Personal records altered without authorisation • Personal records accidentally overwritten • Website defacement • Technical measure not in place to secure personal data.

4. Roles and responsibilities

Position / Group	Description of Responsibility
Senior Information Risk Owner (SIRO) (Executive level with decision making responsibility)	Responsible person who is the allocated lead for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the CEO with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. They will oversee Serious Incidents.
Caldicott Guardian – Regulated by the National Data Guardian not the ICO. (Clinical position executive level with decision making responsibility)	Responsible person within the ICB with overall responsibility for protecting the confidentiality of personal data and special categories of personal data relating to patients (described as Personal Confidential Data (PCD) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the ICB Board and relevant

	committees on confidentiality issues relating to the processing of patient data. They will support the SIRO in overseeing significant incidents (SI). Understands and widely communicates the importance of a positive culture around information assurance.
Data Protection Officer (DPO)/Head of Information Governance (no decision-making powers – should be independent and have expertise in data protection)	Responsible person who has been assigned the responsibilities set out in the UK GDPR, such as monitoring and assuring ICB compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments (DPIA), giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the ICO and members of the public where an individual's rights and freedoms have been breached. The DPO will ensure that where a high-risk incident has occurred, or an individual has complained about the data protection process within the ICB, they will liaise with all parties to come to a solution.
SCW Information Governance Consultant and SCW Information Governance Officer	Will provide support to the CIOS ICB with reporting, investigation and management of information governance incidents and offer advice to ensure the organisation complies with legislation and guidance.
Information Governance Steering Group (IGSG)	Will monitor the compliance of managing information governance incidents against the data protection legislation, NHS data guardian requirements and the Data Security & Protection Toolkit (DSPT). Decision making group on new processes for the management of personal confidential data. Provides oversight for the managing of information governance incidents in line with this procedure and will act as a point of escalation for actions.
Information Asset Owners (IAO)	Identified senior ICB colleagues supporting SIRO by understanding the information they hold and who has access and address risks to the information assets they own. They will ensure incidents are reported, take immediate steps to mitigate the impact of any incident and provide support with the investigation of those incidents.
Information Asset Administrators (IAA)	Will support their IAO and SIRO and work with the IG Team to ensure colleagues apply the Data Protection Legislation and Caldicott Principles within working practices and maintain departmental data flows including detailing any IG incidents.

5. Procedure

This guidance applies to all CIOS ICB colleagues including permanent, temporary and contract staff.

All incidents will be managed in line with the NHS Digital - Guide to Notification of Data Security & Protection Incidents V1.3. Incidents which are determined to have created 'Serious Harm to the rights and freedoms of individuals' will be risk assessed

in line with Recital 87, and if serious harm is identified will be reportable to the ICO, in line with ICO UK GDPR legislation Article 33(5).

If an IG incident is identified or suspected, individuals should immediately notify their Line Manager. The Line Manager must ensure an IG Incident Report Form is completed and forwarded to ciosicb.incidents@nhs.net within 24 hours of identification.

The IG team will receive the IG Incident Report Form and log the incident on the IG Incident Report Log giving the incident a reference number.

Any events having a significant impact on the continuity of essential services must be managed in line with NIS Regulations.

The IG team will assess the incident against the Scoring Matrix to determine the severity of the incident and identify what actions need to be undertaken to manage the incident.

After processing, the IG team will forward the IG Incident Report Form to the reporter and where necessary, the departmental IAO. They will be asked to discuss the breach with their line manager and complete any actions identified, returning the completed IG Incident Form to IG. Where an identified incident has originated in another organisation, this organisation will be notified of the breach and asked to report via their internal mechanisms. If the ICB believes the incident to be serious and the organisation is contracted by the ICB, the organisation will be asked to update the ICB on the steps they have taken to contain the incident and prevent reoccurrence.

If the incident is considered not to be reportable to the ICO, the IG team will continue to manage the incident internally.

If the incident is reportable to the ICO, the IG team will escalate the matter to the Data Protection Officer, SIRO or Caldicott Guardian directly and seek their authorisation to report via the DSPT Incident Reporting Tool within the mandatory 72-hour timeframe. A decision will also be made regarding whether individual data subjects must be contacted under the duty of candour.

In the rare situation that a reportable incident is identified outside of normal working hours, it must be reported to the on call manager who should complete the IG Incident Report Form and contact the DPO. The DPO will consider the seriousness of the breach and decide whether the incident needs to be reported immediately to the ICO to comply with the 72-hour requirement or whether it can wait until the next normal working day. The DPO should report any ICO reportable incidents via the ICB's Data Security & Protection Toolkit. The ICB will ensure that the out of hours process is included with their Business Continuity Plan.

Where applicable, the SIRO, DPO or Caldicott Guardian will jointly determine if the Police or Counter Fraud should also be informed and, where necessary, take steps to report onwards to them.

Where the incident is a result of a cyber event (NIS incident) consideration should be made whether they need to report to the NCSC. The Emergency Preparedness, Planning and Response Team must be contacted for advice and, if necessary, to enact the relevant Action Card.

Where the ICO has been notified, the DPO is the ICB's designated point of contact during the investigation and is responsible for assisting the ICO with their investigation.

6. Reporting

All incidents (Internal and external) will be recorded on the IG Incident Report Log and reported at the IGSG on at least a quarterly basis.

The DPO will report Serious Incidents (SI) to the Executive Team as often as required and will provide a summary at least annually as part of a formal Information Governance Annual Report.

Where an incident has occurred, the IG team will inform the departmental IAA who must ensure that their departmental data flows are updated to identify where a breach has occurred. The provides the IAO with information to review the risk of the data flow/asset and may prompt the review of any associated DPIA, Business Impact Assessment and/or Business Continuity Plan.

A historical record of closed incidents covered by the IG Incident Log will be maintained by the IG team. This is required as DSPT evidence (currently 2 year rolling requirement). Any data included in this record will be held for six months to support any ICO investigation then deleted. The remaining correspondence will be retained for 10 years in line with the Records Management Code of Practice 2023.

7. Training

All colleagues are required to complete mandatory Data Security and Protection Training accessed through the usual statutory and mandatory learning and development portal which includes the importance of incident reporting.

All colleagues will be informed, as part of their induction, of the process for reporting information governance incidents and made aware of the Information Governance pages of the intranet. General awareness will be promoted through newsletter articles and staff briefings. Each colleague also has access to all relevant policies that cover IG.

IAOs and IAAs receive training in their role and duties and can engage with the IG team for further support in their role.

Executive management understand and widely communicate the importance of a positive culture around information assurance.

Following an internal incident the IG team will:

- determine where lessons can be learnt
- ensure that steps are taken to review existing policies, procedures and guidance
- improve relevant security arrangements to prevent further incidents
- recommend where additional training may be required.

IAOs may determine that department Business Impact Assessments or Business Continuity Plans and/or particular DPIA be reviewed.

8. Equality impact assessment

CIOS ICB aims to design and implement services, policies and measures that are fair and equitable. An equality impact analysis has been completed for this procedure and no adverse impact was identified.

9. Monitoring effectiveness

The ICB Information Governance Steering Group (IGSG) will monitor compliance and will assess adherence with this procedure by regular review of the Incident Report Log.

The ICB recognises that failure to comply with this procedure may result in ineffective working and an inability to meet the requirements of Data Protection legislation and the Data Security and Protection Toolkit. Where the procedure is breached, this must be reported to the Data Protection Officer.

10. Distribution

The IG Incident Reporting Procedure will be available and accessible within the Document Library, communicated to all colleagues via the ICB staff intranet.

IAOs will be responsible for ensuring that temporary or contract staff are aware of the correct process to follow if they identify or suspect a breach.

11. Freedom of information requests (foi)

CIOS ICB recognises the need for an appropriate balance between openness and confidentiality in the management of incidents. Incidents will be identified and, where appropriate, kept confidential underpinning the UK GDPR, DPA 2018 and Caldicott principles and the regulations outlined in the Data Protection Legislation and Freedom of Information Act.

Aggregate and non-confidential incident information relating to the ICB and its services will be available to the public through a variety of means including reports, minutes and the procedures established to meet requirements under the Freedom of Information Act 2000. The ICB will follow established procedures to deal with applications from the public.

12. Review

44. This document is reviewed every three years unless organisational changes, legislation or guidance prompt an earlier review. Recurrent instances of non-compliance will be investigated to ascertain the source of non-compliance. If it is found that the policy itself is a source of non-compliance, e.g. is not sufficiently clear, this will trigger a review.

13. References and links to other documents

- Information Commissioners Office (ICO)
- Acceptable Use of IT Policy
- Confidentiality and Safe Haven Policy
- Data Quality Policy
- Freedom of Information Policy
- Information Governance Framework
- Information Security Policy
- Records Management Policy
- EPRR ICB Business Continuity Plan
- Guide to the Notification of Data Security and Protection Incidents
- NIS Regulations 2018
- Data Security and Protection Toolkit

Information Governance Incident Report

Date of incident:	
Time of incident:	
Description of what happened resulting in an information incident (email to wrong address, letter to wrong address, information included in error, information lost, information found, internal information transfer, GP transfer etc):	
What type of information was included (name, address, DOB, NHS number, clinical information, etc):	
How many individuals are included in the information (one individual's information, 5 individuals records, client or staff, member of public, other NHS employee, etc):	
Where did the information come from (internal team/staff, GP practice, other NHS organisation, not know):	
Actions taken (sender informed, advice to report, message deleted, letter destroyed confidentially, apology provided, protocol or process provided for future reference, advice from IG Lead):	

Lessons learned (how could the incident be avoided in the future, is additional training required, do assurances need to be gathered:	
Completed by: **[Name and Job Title]**	
Signed:	
Date:	

Information governance incident scoring matrix

Risk grading descriptions

Likelihood

Score	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence.
2	Not likely	In cases where vulnerable groups involved (even if no adverse effect) or there is no evidence that can prove that no adverse effect has occurred
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Severity

Score	Likelihood	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Minor	Vulnerable groups involved (even if no adverse effect). Where absolute certainty of no adverse effect e.g. cancellation of a procedure (no suffering), Possible inconvenience needing data.
3	Adverse	Confidential data release into public domain leading to embarrassment, cancelled procedure, potential to prolong suffering (but no decline in health).
4	Serious	Where suffering and decline in health has been reported arising from the breach, loss of bank details leading to loss of fund (financial detriment), loss of employment.
5	Catastrophic	A person dies or suffers a catastrophic occurrence.

Risk matrix

Severity (impact) score						
	5 (catastrophic)	**5**	**10**	**15**	**20**	**25**
	4 (serious)	**4**	**8**	**12**	**6**	**20**
	3 (adverse)	**3**	**6**	**9**	**12**	**16**
	2 (minor)	**2**	**4**	**6**	**8**	**10**
	1 (no adverse effect)	**1**	**2**	**3**	**4**	**5**
		1 (not occurred)	2 (not likely)	3 (likely)	4 (highly likely)	5 (occurred)
		Likelihood score Likelihood that citizen's rights have been affected (harm)				

DHSC and ICO

ICO

Data Subject notification and apology letter template

DD MONTH YEAR

[Recipient's name]
[Address line 1]
[Address line 2]
[Postcode]

PRIVATE AND CONFIDENTIAL

Dear [insert recipient's name here]

We are writing to inform you of a data breach that has occurred in relation to your personal data.

[Insert incident details]

I sincerely apologise for this breach and would like to inform you that an investigation has been carried out to find out how this happened. The ICB takes confidentiality very seriously and operates under a culture of being open, honest and transparent where a breach of confidentiality occurs.

[List actions taken to manage this incident]

I understand this may cause some distress, and I would like to reassure you that incidents like this are rare. We have learnt from this incident and are doing what we can to prevent this type of incident happening again.

Should you have any questions or concerns, please do not hesitate to contact us.

Yours sincerely
[INSERT SIGNATURE]

[INSERT DPO/Caldicott Guardian name]
[INSERT TITLE]
CIOS ICB

Appendix 1: Equality impact assessment

Name of policy or service to be assessed: Incident Reporting Procedure
Department or section: Information governance
Date of assessment: 26 March 2025
Person(s) responsible for the assessment: Mike Cottam (SCW CSU)
Is this a new or existing policy? New

Aims, objectives and purpose of the policy

Describe the aims, objectives, and purpose of the policy.
The procedure document outlines the ICB's legal obligations under Data Protection Act 2018 in relation to the management and response process for information governance incidents

Who is intended to benefit from this policy, and in what way?
Policy/procedure is intended for staff and public guidance

What outcomes are wanted from this policy?
To allow for reader understanding of the process that the ICB will follow in the management of its IG incidents and the relevant roles and responsibilities of key staff members involved in that process. An organisational statement of intent to meet its legal obligation to report serious incidents according to legislative requirements. Staff guidance in dealing with incidents.

What factors or forces could contribute or detract from the outcomes?
Failure to meet statutory obligations to report incidents if staff are not aware or do not understand their responsibilities

Who are the main stakeholders in relation to the policy?
Main stakeholders are the ICB and its staff

Who implements the policy, and who is responsible for the policy?
Head of information governance and information governance subcommittee.

Differential impacts

Does this have a positive or negative impact on people from an ethnic minority background? How will any negative impact be mitigated?
There are no differential impacts from this policy as every incident is dealt with in the same way and will follow internal process, regardless of who may be involved. Should there be a need for an individual to liaise in a particular language, format or method, then this need will be met by the organisation wherever possible. Should communications require a specific language, format or method of response, use will be made of translation services available, technology/electronic/hard copy provision of the information and any external guidance available.
Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?

No impact has been identified for this protected characteristic. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of disability? How will any negative impact be mitigated?
There are no differential impacts from this policy as every incident is dealt with in the same way and will follow internal process, regardless of who may be involved. It is recognised that those with a disability may be considered more vulnerable to certain types of breaches and the impact they may have. Due consideration will be given to such individuals and appropriate mitigations in response incidents will be implemented.

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual? How will any negative impact be mitigated?
There are no differential impacts in this policy for people of differing sexual orientation. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
There are no positive or negative differential impacts in this policy for people of any age. It is recognised that elderly individuals may be considered more vulnerable and susceptible to a breach of their information. Every step will be taken as part of incident management response to ensure appropriate reassurances and mitigatory action is implemented. Information can be provided in easy read format if needed or provided in differing languages making use of any translating services needed. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
There are no positive or negative differential impacts in this policy for people of any religion or belief. No negative impact identified.

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies. How will any negative impact be mitigated?
There are no positive or negative differential impacts in this policy for people regardless of marital status. No negative impact identified.

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary, or gender fluid? How will any negative impact be mitigated?
There is no overarching differential impact on people from the perspective of gender re-assignment. No negative impact identified. In the event of a breach involving the data of those individuals who fall within this category, it is recognised that there should be a degree of sensitivity given to the investigation and those affected. Loss of data could cause significant distress and anxiety.

Does this have a positive or negative impact on people who are pregnant, breast feeding mothers, or those on maternity leave? How will any negative impact be mitigated?
There is no differential impact on people from the perspective of pregnancy and maternity. No negative impact identified.

Are they any other identified groups? How will any negative impact be mitigated?
No differential impact on other identified groups has been identified. No negative impact identified to be mitigated.

Human rights values

How have the core human rights values of fairness, respect, equality, dignity, and autonomy been considered in the formulation of this policy, service, or strategy?
Reference to the legislation is included within the document. Data Protection Act 2018 and therefore data subject rights take account of rights under the Human Rights Act Article 8.

Which of the human rights articles does this document impact?

☐ To life
☐ Not to be tortured or treated in an inhuman or degrading way
☐ To liberty and security
☐ To a fair trial
☒ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience, and religion
☐ To freedom of expression
☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☐ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?
Review of the Human rights statement and guidance has taken place and consideration made of the articles.

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?
Reference to the Human Rights Act is contained within the document.

Public Sector Value Act 2012

NHS Cornwall and Isles of Scilly is committed and obliged to fulfil the requirements of the Public Sector Social Value Act 2012. This Act requires the organisations to

consider how services commissioned or procured might improve the economic, social, and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system, and community.
The policy includes the requirement for staff to complete mandatory data security awareness training which increases skills and maintains employment with the ICB. Content of data protection standards ensure that local systems used for processing information are scrutinised and audited for security and integrity.

Describe how the policy contributes towards eliminating discrimination, harassment, and victimisation.
N/A

Describe how the policy contributes towards advancing equality of opportunity.
N/A

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
N/A

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and or the working environment for that group of people.
N/A

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
N/A

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.
N/A

Equality impact assessment action plan

Issue to be addressed	Action required	Responsible person	Timescale for completion	Action taken
N/A	N/A	N/A	N/A	N/A

Comments on action plan:
N/A

Signed (completing officer): Information Governance Consultant (SCW CSU)
Date: 26 March 2025
Signed (head of department or section): Terry Willows, Company Secretary
Date: 24 April 2025