

NENC Secure Data Environment (SDE): Disclosure Control, Output Checking and Release Policy

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 1

Document filename: Report template			
Programme:	Sub National Secure Data Environment – NENC ICB		
Document Ref:	XX		
Programme Director:	Mark Walsh	Status:	Draft
Document Owner:	Marc Rice	Version:	0.5
Author:	Michael Ball	Version issue date:	19/02/2025

Document Management

Revision history

Version	Date	Summary of changes
0.1	23/10/2024	Initial comments
0.2	19/12/2024	Additional comments from SMEs
0.3	24/01/2025	Alignment to NHS E documentation shared (SAIL etc)
0.4	29/01/2025	Minor amendments
0.5	19/02/2025	Clarification on descriptions of egress files

Reviewers

This document has been reviewed by the following people:

Reviewer name	Title/responsibility	Date	Version
Shona Haining	Head of Research & Evidence, NECS	23/10/2024	V0.1
Darren McKenna	Provider Lead, NENC SDE	16/12/2025	V0.2
Arne Wolters	Implementation Lead, NIHR Applied Research Collaboration for the North East and North Cumbria (ARC NENC)	19/12/2024	v.0.2
Vicky Campbell- Molloy & Chris Taylor	Project Support Lead and Principal Technical Architect, NECS	29/01/2025	V0.3
I-Lin Hall and Kim Teasdale	Strategic Head of Digital and Programmes and Head of Analytics	29/01/2025	V0.4
Mark Walsh and Darren McKenna	Provider Lead, NENC SDE and Programme Lead NECS SDE	19/02/2025	V0.5

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 2

Related documents

Title	Owner	Location
Data Access Agreement	NENC ICB	In development
Restricted Output List	NENC ICB	In development
Data Access Request Form	NENC ICB	In development
NENC SDE DPIA	NENC ICB	

Document control

The controlled copy of this document is maintained by the SNSDE NENC programme. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity

List of Abbreviations and Acronyms

Term	Description
SNSDE	Sub National Secure Data Environment
NENC	North East and North Cumbria
MIS	Minimum Information Set
ICB	Integrated Care Board
ORF	Output Review Form
GDPR	General Data Protection Regulation

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 3

Contents

Purpose.....	5
Scope.....	5
Background	5
Key Principles.....	6
Roles and Responsibilities	6
Defining a Safe Output.....	7
Procedure for Output Checking and Removal.....	7
Step 1: Preparation of Output.....	7
Step 2: Submission for Review.....	8
Step 3: Review and Approval	8
Step 4: Documentation and Logging	8
Step 5: Removal from SDE	9
Output release	9
Restricted Output List	9
Appeals process	9
Exceptions.....	9
Compliance and Audit.....	10
Automated checking tools	10
Policy Review	10
References.....	10
Appendices	11
Appendix 1: Output Review Form.....	11
Appendix 2 : Disclosure Control Rules	11
Appendix 3 : Process Flow Diagram	13
Appendix 4 : Data classification types	13
Appendix 5 : Restricted Output List	14

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 4

Purpose

The North East and North Cumbria (NENC) Secure Data Environment (SDE) is a part of the NHS Research Secure Data Environment Network¹. The SDEs are designed to facilitate secure access to health and care data for researchers. The intention is that data will stay within an SDE, however, we know that for the purposes of research (e.g. publishing papers, peer reviews) that some outputs will need to leave the SDE.

The purpose of this policy is to define what the necessary controls are, what can be released and the mechanisms by which the NENC SDE will ensure that all results produced from personal data, and outputs generated and removed from the technical platform, comply with the principle of 'Safe Outputs' as referenced in the UK Data Service Five Safes Framework². The policy establishes procedures to safeguard personal, sensitive or confidential information when outputs are released.

Scope

This policy applies to all users, including researchers, analysts and staff working within the SDE who intend to extract outputs for external use or are charged with disclosure control and output checking. It covers all outputs, including but not limited to; tables, charts, models, code, and reports, and ensures that these outputs adhere to the principle of 'Safe Outputs', before removal from the environment. At present, researchers are only permitted to export results of structured datasets. Outputs such as trained AI models, free-text summaries, or other unstructured data cannot be extracted. As the NENC SDE develops, there will be ongoing work on how different media and file types can be safely removed from the platform.

Background

North East and North Cumbria Integrated Care Board (NENC ICB) is the sole controller for the NENC SDE. As such it has responsibility for overseeing the function of the SDE and is responsible for ensuring that it complies with agreed standards.

As part of a network of SDEs, it is expected that the NENC SDE will comply with standards set out by NHS England as part of an accreditation scheme. These requirements have not yet been confirmed. The NENC SDE has therefore developed a local output checking policy in the interim. It is expected that further national guidance will be provided and alignment with others NHS SDEs. This policy will be reviewed in light of any such accreditation. The current policy does reference and include principles set out by the National NHS England SDE³. It has also taken into consideration policies and positions of other Secure Data Environments such as Genomics England and SAIL.

¹ <https://digital.nhs.uk/data-and-information/research-powered-by-data/sde-network>

² <https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/>

³ <https://digital.nhs.uk/services/secure-data-environment-service>

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 5

Key Principles

The following principles will be the basis of the NENC SDE policy:

- **Output**
 - For the purposes of this document, an output is a data item that is being requested to be removed from the secure data environment.
- **'Safe Outputs'**
 - Consideration will be given to what will be released, the confidential nature of the information, the risk that it could be used to identify somebody and mitigation and minimisation of the risk.
 - This is essentially a risk management policy, not a risk elimination policy which will broadly follow a 'principles-based' approach with 'rules-based' ⁴ elements, where more appropriate.
- **Compliance with Data Policies:**
 - Outputs must comply with any relevant data-sharing agreements or protocols.
 - Users must ensure outputs do not contain any personal data as defined by UK GDPR.
- **Review and Approval:**
 - Every output must be reviewed and approved by the designated Data Output Reviewer before it can be removed from the SDE.

Roles and Responsibilities

- **Researcher:**
 - Ensure all outputs comply with the principle of 'Safe Outputs'.
 - Submit the output for review using the designated process, including the provision of an Output Review Form (ORF) to the SDE Administrator.
- **Data Output Reviewer:**
 - Review the submitted output for compliance with the principle of 'Safe Outputs'.
 - Approve or reject the output based on compliance with the policy.
 - Document the review and approval/rejection process.
- **SDE Administrator:**
 - Provide ORF to Researcher for completion in advance of submission and ensure completion in compliance with the policy.
 - Facilitate the review process and ensure that outputs are securely transferred if approved.
 - Maintain logs of all outputs approved, referred or rejected and their corresponding review documentation.

⁴https://www.google.com/url?sa=i&url=https%3A%2F%2Fukdataservice.ac.uk%2Fapp%2Fuploads%2Fthf_datareport_aw_web.pdf&psig=AOvVaw0--XDUO1RisCijSwOpRZSc&ust=1729698343878000&source=images&cd=vfe&opi=89978449&ved=0CAcQr5oMahcKEwjw-KPMqqKJAxUAAAAHQAAAAQBA

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 6

- **NENC ICB**

- As the Sole Controller of the NENC SDE, the ICB is responsible for overseeing the NENC SDE and ensuring compliance with any standards or accreditation. The ICB via the NENC Data Access Committee (DAC), will receive reporting on the numbers of outputs shared and instances where researchers have attempted to act deliberately in contradiction to this policy. The DAC will also have visibility at the outset of projects what the proposed outputs will be and have the opportunity to make recommendations and stipulations on the project.

Defining a Safe Output

To enable researchers to comply with this policy, clear guidance needs to be provided as to what constitutes a safe output. For the purposes of the NENC SDE, the following must apply:

- No personal data can be removed from the SDE
- Results must be aggregated – no individual level data should be included
- Suppress all counts under 10 (this also includes numbers of observation included in a derived statistic)

Further detail is provided on this in Appendix 2. As the NENC SDE develops, examples of safe outputs will be shared with researchers as part of the user guide when they first access the SDE. This will help support users to think about the outputs they will create at the start of their project.

Researchers should ensure that they follow these principles before making an export request to the SDE. Failure to do so will result in a delay to export requests.

As part of the initial application to the NENC DAC, prospective projects will be expected to define what their expected outputs are. Although there is an appreciation this may change during the course of the research, it is expected that the DAC would review and provide feedback on this aspect of the application and raise any risks, concerns or stipulations at this part of the process which would need to be considered when reviewing the output.

In some cases, Data Providers may stipulate that additional requirements or restrictions are placed on the outputs of research from the data they provide. Where this is the case, the NENC SDE will log these requirements and make this known to researchers and the DAC at the outset of the project. Output reviewers will apply these requirements in addition to the normal requirements outlined in this policy.

Procedure for Output Checking and Removal

Step 1: Preparation of Output

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 7

- Researchers must complete an ORF (see Appendix 1) in advance of submission.
- Ensure that all outputs comply with the Disclosure Control Rules (Appendix 2)
- Ensure any graphs and other visualisations are clearly labelled to show what they represent.
- Place the relevant export file in the Export" folder on the workspace desktop.

Step 2: Submission for Review

- Email the ORF to nencicb.sde@nhs.net for review

Step 3: Review and Approval

- The Data Output Reviewer will:
 - Check the output for compliance with the principle of 'Safe Outputs' utilising where appropriate and available, automated tools. (Technical appendix – to be developed as automate checking is included)
 - Ensure there is no data that could be constrained as personal / restricted data by checking against the principles of the Disclosure Control Rules and the Restricted Output List (Appendix 5)
 1. Cross-reference against the database of previous output release requests
 2. Cross-reference against the Data Access Agreement and any feedback from the DAC
 3. Assess the risk of Attribution and Secondary Disclosure. (REF)
 - Review the methodology used for ensuring compliance.
- The Reviewer will approve the output if it meets the required standards based on the principle of risk-management, reject it, or refer it back to the Researcher with feedback for necessary modifications.
- Secondary review/sign-off – For outputs or projects where data is categorised as Person identifiable – very sensitive (Appendix 4), the review process should involve two, separate reviewers, at least one of which was not involved in any analysis of the data, checking independently and then a consensus on whether to release will be produced. This second reviewer would need to be impartial and independent.

Step 4: Documentation and Logging

- For all outputs, the Reviewer will document the review process, including details of
 - All outputs requested.
 - Reviewer's decision (i.e. output released, rejected, 'referred' or withdrawn)
 - Details of who requested the outputs

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 8

- Details of who checked and reviewed the request
 - Details of any issues or amendments requested/applied
 - The reasoning behind each decision
 - The date when the request was made, approved, and outputs released.
- The SDE Administrator will log the requested output and maintain records of all outputs and reviews in a database. As part of the NHS E SDE network, this will align to agreed national standards in the longer term. While these are in development, NENC SDE will agree a consistent format.
 - It is important that the naming convention is easy to understand and will facilitate future checking to minimise Attribution & Secondary Disclosure etc.

Step 5: Removal from SDE

- Once the output is approved, the SDE Administrator will facilitate its safe, secure transfer to the requester's designated location.
- Any issues or discrepancies during transfer must be reported and resolved before the output is considered released.

Output release

Standard output requests will be reviewed within 5 working days. More complex requests may extend beyond this. If the output is safe, this will be provided to the researcher by email. If it is deemed that the output does not meet the requirements, the request will be rejected and the researcher will receive an email informing them of the reason why.

Each research workspace should request no more than 5 outputs a week. If a workspace submits more than 5 files, any extra files may not be assessed until a decision on the initial release request has been made.

Restricted Output List

Some datasets may have additional restrictions from either the SDE or from the data providers. These requirements will be maintained in the Restricted Output List (appendix 5) and all outputs will be checked against this.

Appeals process

If a researcher does not agree with the decision of the Data Output Reviewer, they can appeal this decision by emailing nencicb.sde@nhs.net. The decision will then be reviewed by an alternative Data Output Reviewer for a secondary opinion.

Exceptions

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 9

Exceptions to this policy will only apply if the specific output has been approved by the Data Access Committee and there is a relevant legal basis for the disclosure.

Compliance and Audit

- Regular, continuous audits, both internal and external will be conducted to ensure adherence to this policy, the review process and outputs released are consistent over time and are aligned with the aims and goals of the SDE.
- All outputs reported from the NENC SDE must be requested out via the output review process. Even small outputs, such as a single number that a researcher may easily remember and write down, should be requested via the output review process, so that all outputs are documented, and that both the NENC SDE and the researcher have confidence that the output is safe.
- Any breaches or attempts to circumvent this policy will be reported to the appropriate authority and may result in disciplinary action, including suspension of SDE access. It is anticipated that once established this will be the NHS England User and Organisation Validation Committee.

Automated checking tools

The use of automated or semi-automated tools to perform checking of outputs will be explored in the future. As the use of the SDE and demand for outputs increases, this will be necessary.

Policy Review

This policy will be developed over time and as a result of learning from the initial stages of operation but as a minimum, it will be reviewed annually or as required by changes in legislation, data-sharing agreements, or operational requirements.

References

Further information can be found in the following :

- [SACRO Output Checking Guide](#)
- [SAIL Output review policy](#)
- [Genomics England Air Lock](#)
- [LSE TRE Egress Documentation](#)
- [NHS England Output Rules](#)
- [UK Data Service Handbook on Statistical Disclosure Control](#)

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 10

Appendices

Appendix 1: Output Review Form

1. **Researcher Name:**
2. **Project reference number:**
3. **Department/Team:**
4. **Email Address:**
5. **Date of Submission:**
6. **Name of output file:**
7. **Description of Output:**
(Briefly describe the content and purpose of the output.)
8. **Intended Use of Output:**
(State how the output will be used outside the SDE.)
9. **Methodology used to ensure 'Safe Outputs':**
(Describe the method used:)
 - Document which Datasets were used within each output
 - Sample selection criteria
 - Methodology – i.e. suppression, aggregation, tables, charts, maps, residual plots, regression coefficients etc
 - Description of variables
 - Description of results
10. **Confirmation of Compliance:**
(Tick box) I confirm that to the best of my knowledge and understanding, this output complies with the NENC SDE Disclosure Control, Output Checking and Release Policy.
11. **Reviewer Comments:**
(For use by Data Output Reviewer during review.)
12. **Review Decision:**
 - Approved
 - Rejected (provide reasons)
 - Referred (with details of requested amendments)
13. **Reviewer Name:**
14. **Reviewer Signature:**
15. **Date of Review:**

Appendix 2: Disclosure Control Rules

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 11

Requested results must:

- Be aggregated, summary results
- Suppress all counts under 10 (for example where a result of 7 is recorded, this should be shown as “*”). Where the result is 0, a 0 can be shown but would need to be checked in the context of the output and a justification of why this should be included.
- Ensure suppressed numbers cannot be calculated through use of other information (such as total and sub-total values)
- Graphs and other visualisations are treated the same as numeric results, where exact values can be determined
- Contain only data that would be appropriate to make available in the public domain (for example in a research paper or report)
- Data output spreadsheets should not contain hidden text/data/tabs or data in document properties/metadata
- Not contain any data included in the Restricted Output List

Requested data outputs:

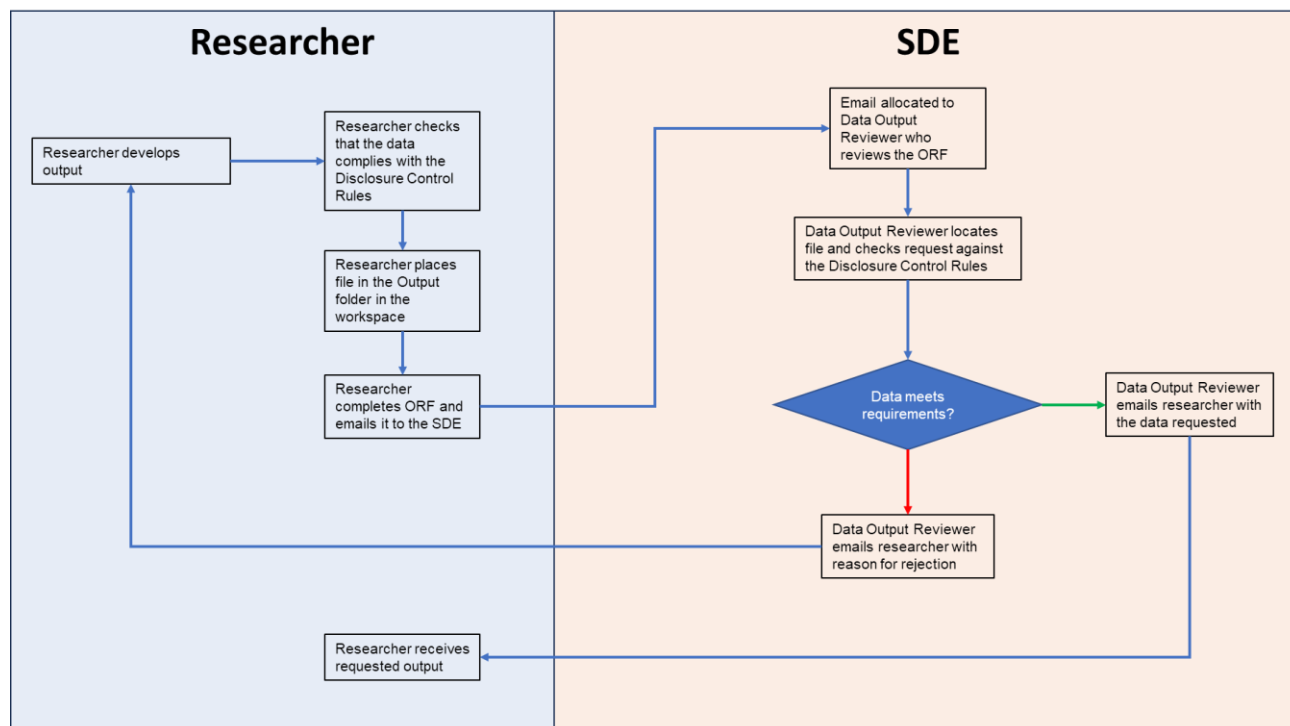
- Should ideally not exceed 1,000 rows or 30 columns. This is to ensure that the requested output can be manually checked by the Output Checking team
- **Must not** contain personal or commercially sensitive data. If an output does exceed this you must contact the SDE team to discuss this request in more detail.

Requested free text outputs (including code) **must not**:

- Include any personal data within the software source code or embedded comments
- Include any commercially sensitive data (explicitly or implicitly) within the software source code or embedded comments

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 12

Appendix 3: Process Flow Diagram



Appendix 4: Data classification types

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 13

Categorisation of data stored within SDE workspaces is included below. These are referenced in the NENC SDE DPIA.

Classification	Example
Public Domain Data	non-person data that is freely accessible eg. mapping data, weather etc
Non-person restricted	non-person data, including aggregate data but not freely available and potentially commercially licensed/restricted
Person identifiable – sensitive	this would be the majority of the data in the SDE eg, health and care data, potentially other data such as police data etc. in the future
Person identifiable – very sensitive	similar to above but this data is usually subject to additional restrictions/regulation within the health and social care or other sector eg. child protection information, gender identity, HFEA data, sexual health etc

Appendix 5: Restricted Output List

Document Owner: Marc Rice	Prepared by: Michael Ball	First Published: 19/02/2025
Document number: 0.5	Issue/approval date: 28/02/2025	Version number: 0.5
Status: Approved	Next review date: 28/02/2027	Page 14

Dataset	Description	Data Provider specific? (Yes/No)	Provider ODS code