

NESO's Data Classification and Sharing processes

Simon Morris – NESO Data Sharing Lead

GC0181 Workgroup

18/2/2026

Information Ringfencing – the NESO licence outlines obligations that NESO employees, contractors and 3rd parties have to protect and improve NESO's data. We must also comply with Ofgem data best practice



Classify data in accordance with NESO's data classification policy



Ensure data is shared in accordance with NESO's data sharing policy



Report a data quality problem so that it can be investigated and prioritised

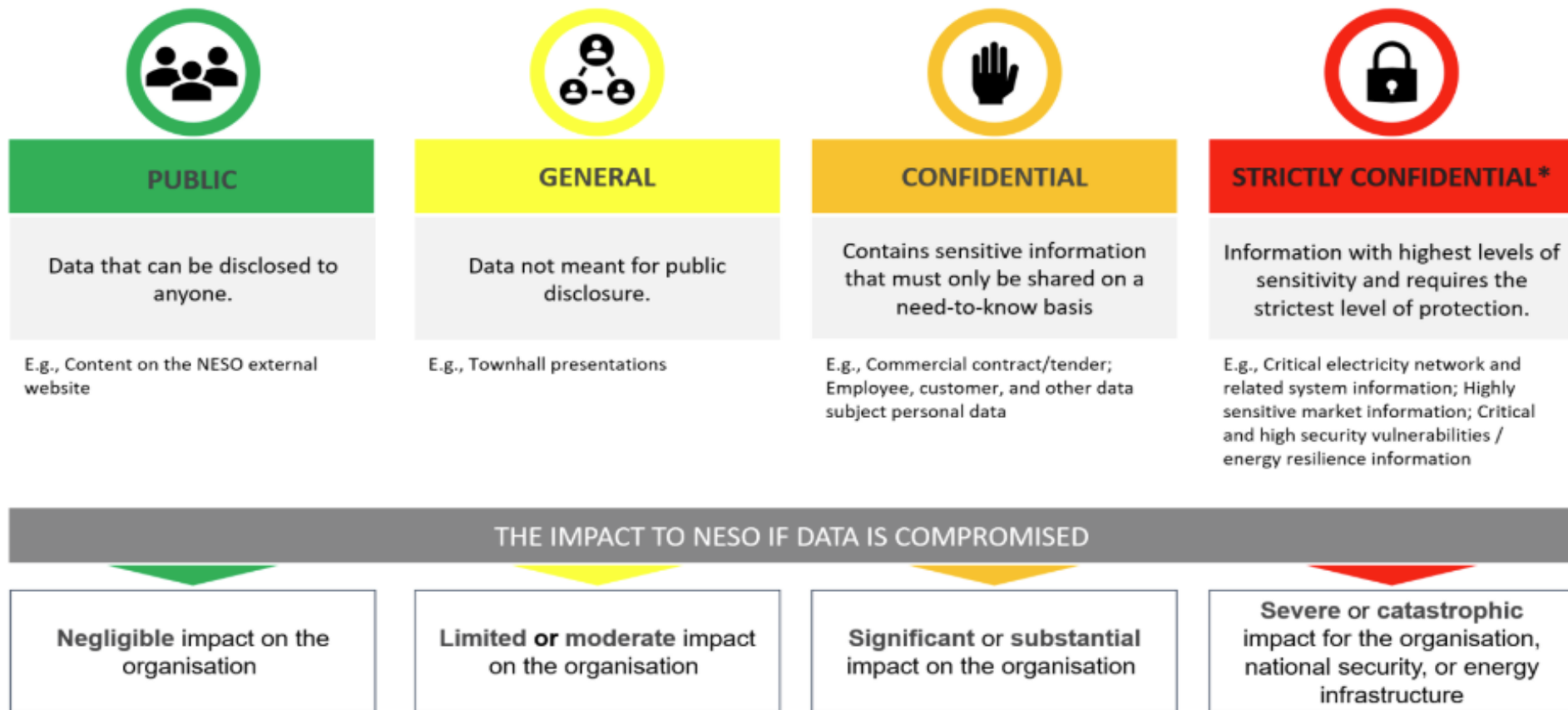


Request a Data Privacy Assessment when handling personal data for a new purpose

Data Classification – the process of categorising and managing information assets based on its sensitivity, importance, and value to the organisation. It involves assigning labels or tags to indicate their level of confidentiality, integrity, and availability.

Data Classification Framework

This is a Data Governance framework that organises data or information into different levels of confidentiality based on data content.



Data Classification – additional guidance is provided on how we determine the level of confidentiality

Sensitive Data Category	Examples	Classification guidance
Personal data	Non-NESO email address	• CONFIDENTIAL
Sensitive Personal data	Age, Race, Religion	• STRICTLY CONFIDENTIAL
Information Request Notice data	Smart washing machine energy usage	<ul style="list-style-type: none"> • DEPENDS ON NATURE OF THE DATA <ul style="list-style-type: none"> ◦ Use your judgement, based on the harm that could be caused should the data be inappropriately shared, what the contract terms are (if any) and what security measures would be needed to protect it.
Not NESO data	Bidding information	
Third Party data	Purchased data subject to contract	
Legal	Information pertaining to an ongoing police or legal investigation.	<ul style="list-style-type: none"> • CONFIDENTIAL unless: <ul style="list-style-type: none"> ◦ Unauthorised disclosure could place NESO in material breach of laws, contracts or regulation in which case it is STRICTLY CONFIDENTIAL
Market or Commercially Sensitive data *	Prequalification outcomes prior to be released externally, bidding information, clearing prices, commercial tender information, business plans	<ul style="list-style-type: none"> • CONFIDENTIAL unless: <ul style="list-style-type: none"> ◦ Unauthorised disclosure could expose the energy market to material risk of price manipulation ◦ Unauthorised disclosure could bestow a commercial or competitive advantage to recipients in which case it is STRICTLY CONFIDENTIAL
Energy Resilience data *	Energy risk and threat advice, post-event and post-emergency analysis, the Energy Resilience Assessment Report, the Emergency Processes Assessment, the Industry Readiness and Preparedness Report	<ul style="list-style-type: none"> • CONFIDENTIAL unless: <ul style="list-style-type: none"> ◦ Unauthorised disclosure could put the energy resilience or energy security of the country at material risk in which case it is STRICTLY CONFIDENTIAL
Additional Ringfenced data (CNI, National Security) *	RFU IP Addresses, server names, system restoration plans, energy sector risk assessments	<ul style="list-style-type: none"> • CONFIDENTIAL unless: <ul style="list-style-type: none"> ◦ Unauthorised disclosure could put the national security of the UK at material risk in which case it is STRICTLY CONFIDENTIAL

*Ringfenced under NESO licencing obligations

Data Classification – the data classification will then outline the way in which the data or information should be stored, who can access, how we distribute and how we physically secure it



GENERAL

Storage

- Don't store documents on local drives – use a shared drive or a SharePoint

Access & Distribution

- Documents should not be shared by copy – a link should be provided instead
- Information must not be sent to external recipients, unless authorised

Physical Security

- Laptops must be screen locked when the user is not in attendance
- Printed documents must not be left lying on desks



CONFIDENTIAL

In addition to (or in case of conflict, superseding) the above:

Storage

- Store data in limited access folders / repositories. OFFICIAL documents received from government must be stored in designated folders in limited access SharePoint or shared drives

Access & Distribution

- Share links to documents, and only on a need-to-know basis - use the 'Share' menu bar option to manage access
- Use passwords if it is only practicable to share copies of documents
- Don't put copies of Confidential documents on Teams chat

Physical Security

- Keep printed information and removeable media locked away
- Take measures to ensure conversations cannot be overheard e.g. behind closed doors



STRICTLY CONFIDENTIAL*

In addition to (or in case of conflict, superseding) the above:

Access & Distribution

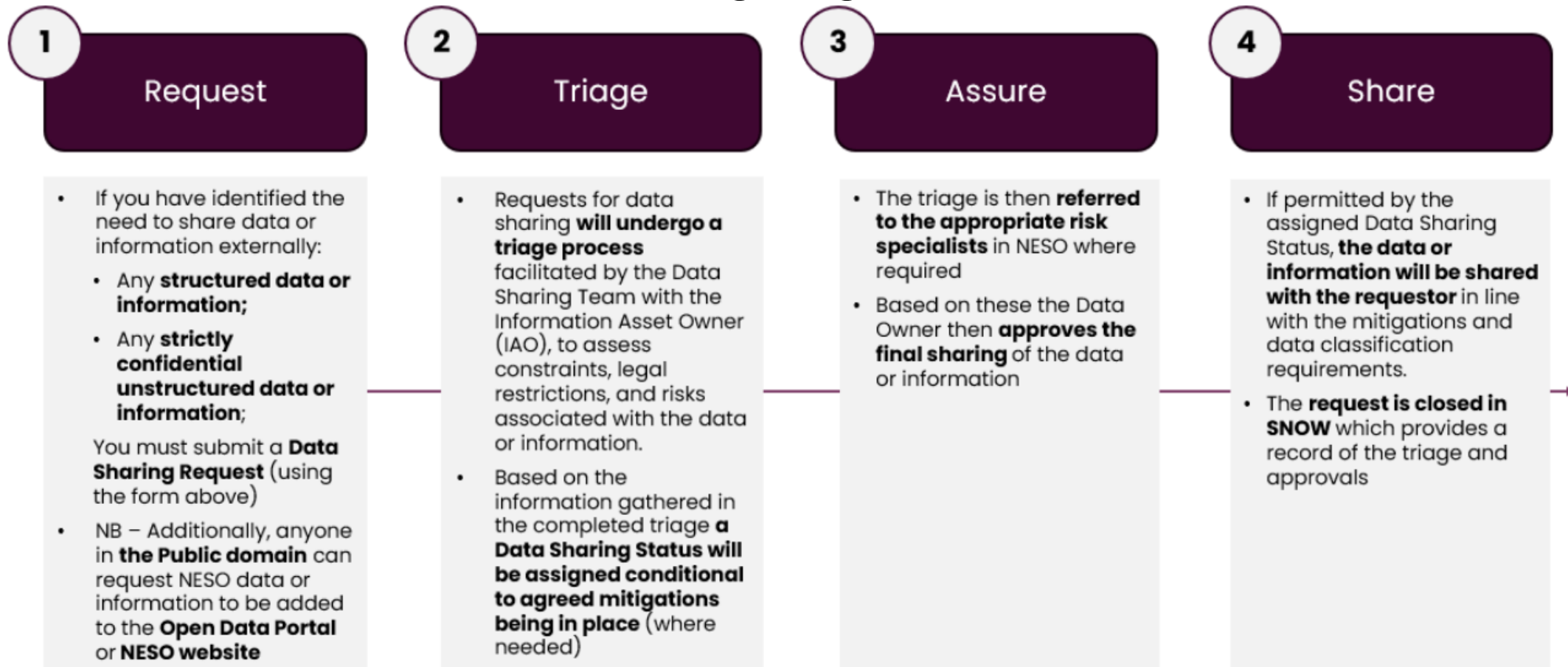
- Only access data from private areas that cannot be overseen
- Only share on a strict need-to-know basis, to an approved distribution list of named individuals
- Remove access when no longer required

Physical Security





- Only access printed information and removeable media in approved areas
- Only have conversations in approved areas

Data Sharing – is the process of securely and responsibly transferring information assets from NESO to external parties outside the organisation. This involves following specific conditions and guidelines to ensure security, privacy, and compliance with relevant laws and regulations.

Data Sharing Triage Process



Data Sharing Statuses – as a result of the triage process a data sharing status is applied to the dataset which defines who the data can be shared with and how it is shared

				
	OPEN	PUBLIC	SHARED	CLOSED
DESCRIPTION	Data or information is made available for all to use , modify and distribute with no restrictions. <i>Example: Daily Wind Availability Data</i>	Data or information is made publicly available but with some restrictions on usage e.g. it cannot be shared in an adapted form. <i>Example: Research Article on NESO website</i>	Data or information is made available to a limited group of participants possibly with some restrictions on usage. <i>Example: Balancing Information to industry parties</i>	Data or information is not available to share outside on NESO. <i>Example: Energy Resilience Plans</i>
HOW TO SHARE	Can be shared via any means including the Data Portal, NESO website or emails.	Can be shared via any means including the Data Portal, NESO website or emails, however the license conditions must be stipulated .	Can only be shared via a mechanism that is in line with the classification of the data . Tools such as Egress and External SharePoint sites can be used.	Not Applicable

