



FAIRsFAIR
Fostering Fair Data Practices in Europe

FAIR-enabling Data Policy Checklist

The FAIRsFAIR landscape assessment¹ found that data policies that are clear and easy to understand can positively influence researchers in making their data FAIR. This checklist is based on FAIRsFAIR's policy enhancement recommendations² and will help users assess whether specific elements of their data policies are FAIR-enabling as well as providing recommendations for good practice.

The checklist is broken into three sections each dealing with a different aspect of the policy. These include:

- **Context** of the policy such as the title and the year the policy came into effect
- **Content** of the policy focusing on suggested and required aspects of RDM and data sharing
- **Support** for adhering with the policy and **compliance** monitoring

Using the checklist

Users of this checklist should work through the list of policy elements included under each of the three sections and select the option that best reflects the content of their current or draft data policy. Please note, the majority of policy elements presented in this checklist are assessed as either being FAIR-enabling (green) or not (red). For some elements, there is a third option which indicates that the element may enable FAIR to some degree but lacks sufficient rigour or clarity.

Benefits

Using the checklist helps policy makers to easily identify specific policy elements that are not FAIR-enabling and can be helpful in prioritising aspects that may need to be amended in future policy reviews and updates.

¹ Davidson, Joy, Engelhardt, Claudia, Proudman, Vanessa, Stoy, Lennart, & Whyte, Angus. (2019). D3.1 FAIR Policy Landscape Analysis (v1.0). FAIRsFAIR. <https://doi.org/10.5281/zenodo.5537032>

² Davidson, Joy, Grootveld, Marjan, Whyte, Angus, Herterich, Patricia, Engelhardt, Claudia, Stoy, Lennart, & Proudman, Vanessa. (2020). D3.3 Policy Enhancement Recommendations (1.0). Zenodo. <https://doi.org/10.5281/zenodo.5362183>

Interpreting the results and reaching consensus

We recommend that two or three people carry out the assessment of the selected data policy using this checklist. We highly recommend including not just those who are involved in developing or supporting the data policy but those who need to comply with the policy as well.

- **Green** - indicates that the policy element is FAIR-enabling and provides sufficient clarity to enable researchers to understand what is expected of them.
- **Yellow** - indicates that the policy element may be FAIR-enabling to some degree but greater rigour and/or clarity may be needed.
- **Red** - indicates the policy element is either not addressed or does not enable FAIR practice.

Where there are areas of disagreement on the assessment of specific policy elements, we recommend that these be explored collectively to identify why there are differing views. This approach helps to ensure that you reach a consensus view on each of the policy elements and can help to highlight areas where the policy may lack clarity.

Context of the FAIR-enabling Data Policy

This section contains details about the context of the policies themselves such as the title, year of introduction and associated persistent identifiers.

Policy element	Good practice recommendation	Tick the statement that best reflects your policy	
Title of the policy	To support findability, policies should have a title that makes clear whose policy it is and what the policy relates to.		<ul style="list-style-type: none"> The policy has a clear and appropriate title.
			<ul style="list-style-type: none"> The title of the policy would benefit from being made more explicit.
			<ul style="list-style-type: none"> The policy does not have a title.
Year the policy was introduced	To support both human interpretation and machine actionability, the policy should make clear the period of validity, differentiating between the date it was written and the date it was implemented where necessary.		<ul style="list-style-type: none"> The policy clearly states when it came into effect and provides a scheduled review date.
			<ul style="list-style-type: none"> The policy clearly states when it came into effect but does not provide a scheduled review date.
			<ul style="list-style-type: none"> The policy does not make clear when it came into effect or provide a scheduled review date.
Persistent Identifier (PIDs) of the policy document	PIDs should be assigned to clearly versioned policies to ensure that the right version can be found and fed into machine actionable pipelines.		<ul style="list-style-type: none"> The policy has a persistent identifier such as a DOI.
			<ul style="list-style-type: none"> The policy does not have a persistent identifier such as a DOI.
Policy is registered	Policies should be registered with services such as FAIRsharing or similar to improve their findability for various end users.		<ul style="list-style-type: none"> The policy is registered with one or more registry services
			<ul style="list-style-type: none"> The policy is not registered
Availability of the policy	Policies should be openly available and described consistently using a structured data markup schema to support both human and machine readability.		<ul style="list-style-type: none"> The policy is openly available online in a structured format.
			<ul style="list-style-type: none"> The policy is openly available online (e.g., HTML, PDF).
			<ul style="list-style-type: none"> The policy is not openly available online.

Content of the FAIR-enabling Data Policy

This section focused on characterising the scope and the content of the policies.

Policy element	Good practice recommendation	Tick the statement that best reflects your policy	
Scope of the policy	The policy should provide a clear definition on the range of outputs that are covered by the policy such as publications, research data and software.	Green	<ul style="list-style-type: none"> The policy makes clear the range of outputs that are covered and which are not in scope.
		Red	<ul style="list-style-type: none"> The policy lacks clarity on which research outputs are covered.
Definition of research data	The policy should provide a clear definition of what is meant by the term research data which can cover a very broad range of output types.	Green	<ul style="list-style-type: none"> The policy provides a clear definition of what is meant by the term research data.
		Red	<ul style="list-style-type: none"> The policy lacks clarity over what is meant by the term research data.
Research software	The policy should make clear that research software required for reproducibility is deposited with a suitable code repository.	Green	<ul style="list-style-type: none"> The policy provides clarity on expectations for handling research software.
		Red	<ul style="list-style-type: none"> The policy lacks clarity on expectations for handling research software.
Data sharing	The policy should require data sharing unless there are valid reasons not to share the data. The policy should also make clear which exceptions to data sharing are allowed (e.g., personal sensitive, commercial sensitivity). Any embargo periods that are allowed should be clearly stated in the policy.	Green	<ul style="list-style-type: none"> The policy clearly states that data sharing is required and provides clarity on legitimate exceptions to data sharing.
		Yellow	<ul style="list-style-type: none"> The policy encourages data sharing.
		Red	<ul style="list-style-type: none"> The policy does not address data sharing.
Alignment with FAIR (Findable, Accessible, Interoperable, Reusable) Principles	Policies should align with the FAIR principles. Whether the FAIR Principles are referred to explicitly or implicitly in the policy is less important than whether the practical requirements relating to FAIR (sharing, depositing with repositories, etc) are clearly outlined in the policy.	Green	<ul style="list-style-type: none"> The policy makes explicit reference to the FAIR Principles and aligns with FAIR.
		Yellow	<ul style="list-style-type: none"> The policy does not specifically refer to the FAIR Principles but aligns with FAIR.
		Red	<ul style="list-style-type: none"> The policy does not address the FAIR Principles explicitly or implicitly.
Metadata sharing	The policy should make clear any expectations around metadata sharing in particular when the data cannot be shared openly or if	Green	<ul style="list-style-type: none"> The policy clearly states that sharing metadata for selected data outputs is required.

	<p>data are no longer accessible. An emphasis should be placed on making clear whether metadata sharing is required or is suggested.</p> <p>Conditions for access should also be made clear in the metadata records of the deposited dataset. Policies should require tombstone metadata records be maintained after the data may no longer be available to avoid dead ends (e.g., data is destroyed after a retention period).</p>	<p>Yellow</p> <p>Red</p>	<ul style="list-style-type: none"> The policy encourages metadata sharing but does not require it. The policy does not address metadata sharing or lacks clarity over what is expected of researchers when it comes to sharing metadata.
Data Management Plan (DMP)	Data management planning is an essential first step in the research lifecycle and ensures that researchers and data stewards can plan effectively to make research data findable, accessible, interoperable and reusable (FAIR). Policies should require the development of a DMP as part of research practice.	Green	<ul style="list-style-type: none"> The policy requires the development of a data management plan.
		Yellow	<ul style="list-style-type: none"> The policy encourages the development of a data management plan.
		Red	<ul style="list-style-type: none"> The policy does refer to data management plans.
Timing of DMP	Where DMPs are required, policies should provide clarity over the timing of their preparation and delivery (pre award, in award, post award). If multiple versions are required at different stages, this should be made clear.	Green	<ul style="list-style-type: none"> The policy makes clear at what stage the DMP should be prepared.
		Yellow	<ul style="list-style-type: none"> The policy lacks clarity about when the DMP should be prepared.
		Red	<ul style="list-style-type: none"> The policy does not include an expectation for a DMP .
Updating of DMP	It is advisable that the policy includes an expectation that DMPs will be updated over the research lifecycle. Updated DMPs should be clearly versioned.	Green	<ul style="list-style-type: none"> The policy makes clear that the DMP should be updated over the life of the project.
		Red	<ul style="list-style-type: none"> The policy lacks clarity about whether the DMP should be updated.
Data Protection	Policies should make clear any expectations associated with data protection legislation such as GDPR or similar.	Green	<ul style="list-style-type: none"> The policy makes clear that data protection is part of research data management and provides links to related policies and/or supporting documentation.
		Yellow	<ul style="list-style-type: none"> The policy refers to data protection but does not provide links to related policies and/or

			supporting documentation.
			<ul style="list-style-type: none"> The policy does not refer to data protection.
Research integrity	It is advisable that policies and/or related guidance emphasise that data management planning and sharing data supports research integrity goals, enhances data quality and contributes to reproducibility and transparency.		<ul style="list-style-type: none"> The policy makes reference to research integrity as part of research data management.
			<ul style="list-style-type: none"> The policy does not clearly reference research integrity as part of research data management.
Reference to standards	Policies should encourage researchers to make use of existing generic and/or domain specific standards or protocols wherever possible.		<ul style="list-style-type: none"> The policy clearly encourages the use of generic, domain and/or community standards or protocols.
			<ul style="list-style-type: none"> The policy does not encourage the use of generic, domain and/or community standards or protocols.
Repositories	Policies should provide clarity about where research outputs should be deposited. We recommend requiring that trusted digital repositories should be used wherever possible, providing a definition of what this term means and guidance on suggested repositories that may be used.		<ul style="list-style-type: none"> The policy requires the use of trusted digital repositories.
			<ul style="list-style-type: none"> The policy recommends using trusted digital repositories.
			<ul style="list-style-type: none"> The policy does not address the use of trusted digital repositories for data deposit.
Data Availability Statement	Policies should make clear that Data Availability Statements are provided in publications indicating how to access the underlying data or how to request legitimate access to closed data.		<ul style="list-style-type: none"> The policy makes clear that a Data Availability Statement is required.
			<ul style="list-style-type: none"> The policy encourages the provision of a Data Availability Statement.
			<ul style="list-style-type: none"> The policy does not refer to Data Availability Statements.
Intellectual Property (IP)	Policies should refer to Intellectual Property.		<ul style="list-style-type: none"> The policy addresses IP.
			<ul style="list-style-type: none"> The policy lacks clarity over IP.
Licences	Policies should require the use of appropriate licences making clear what reuse conditions (if any) must be respected.		<ul style="list-style-type: none"> The policy requires the use of appropriate licences for research outputs.
	Related policy guidance should be		<ul style="list-style-type: none"> The policy encourages the use of appropriate licences for research

	provided to help researchers to select appropriate licences.		outputs.
			<ul style="list-style-type: none"> The policy does not refer to licences.
Data Citation	Policies should include a clear statement in relation to data citation expectations. Related guidance should provide advice on how to cite a broader range of research outputs including data and software, as well as actors and enablers such as data managers, data stewards, funding bodies, research infrastructures and organisations.		<ul style="list-style-type: none"> The policy provides a clear expectation about data citation.
			<ul style="list-style-type: none"> The policy lacks clarity in relation to expectations around data citation.
Researcher Identifiers	The use of researcher identifiers (e.g., ORCID) should be required to support the overall FAIRness of data outputs by enabling them to be linked unambiguously to specific researchers.		<ul style="list-style-type: none"> The policy requires the use of researcher identifiers.
			<ul style="list-style-type: none"> The policy lacks clarity over the use of researcher identifiers.
Preservation	The policy should make clear the period of time beyond the life of the project that selected outputs must be retained.		<ul style="list-style-type: none"> The policy requires that selected data must be preserved for a set period of time.
	Links to relevant preservation policies and/or retention schedules should be provided.		<ul style="list-style-type: none"> The policy lacks clarity in relation to the preservation of selected data.
	Guidance should be provided to assist researchers to assess the potential risks, benefits and associated costs to enable the preservation of FAIR data over time as they draft their DMP.		

Support for the FAIR-enabling Data Policy

This section contains details about the support provided to enable researchers to adhere with the policies.

Policy element	Good practice recommendation	Tick the statement that best reflects your policy	
Costs	Funding bodies' data policies should support justified costs associated with RDM and making data FAIR.		<ul style="list-style-type: none"> The policy supports justified costs associated with RDM and making data FAIR.
			<ul style="list-style-type: none"> The policy lacks clarity over whether justified costs associated with RDM and making data FAIR will be supported.
Costs	Research Performing Organisations' policies should encourage researchers and support staff to collectively identify relevant costs that should be requested in grant applications through the development of a data management plan.		<ul style="list-style-type: none"> The policy makes clear that justified costs associated with RDM and making data FAIR should be identified through the development of a pre-award DMP.
			<ul style="list-style-type: none"> The policy does not address how justified costs associated with RDM and making data FAIR should be identified.
Guidance	Policymakers should provide access to generic guidance to help researchers to comply with their policies. Where relevant and where resources allow, policymakers should provide access to domain specific guidance.		<ul style="list-style-type: none"> Associated guidance is provided to help researchers to adhere with the policy.
			<ul style="list-style-type: none"> It is not clear whether associated guidance is provided to help researchers adhere with the policy.
Monitoring	Policies should make clear how and when compliance will be monitored. If monitoring will take place, rewards for compliance and/or penalties for non-compliance should be made clear.		<ul style="list-style-type: none"> The policy makes clear whether compliance will be monitored and provides clarity on related rewards or penalties.
			<ul style="list-style-type: none"> The policy does not address monitoring or lacks clarity over whether compliance will be monitored.