UNIVERSITÀ DI MACERATA

Research Security and Integrity:

University Policy

Table of Contents

Introduction **2**

Definitions **2**

Parties Addressed by this Policy **3**

Context **4**

Research Security and Integrity: The SSH Disciplines **5**

Building a culture of research security and integrity (2026-2029) **6**

1. Awareness-raising and Information **7**

2. Support and Advice **7**

3. Promotion of Good Practice in Research Management **7**

4. Gradual Approach to Developing Self-Assessment Tools **8**

5. Monitoring and Progressive Updating **8**

References **9**

Introduction

This document responds to European and national recommendations that call on universities to adopt policies and guidelines for managing research security and integrity, amid a global landscape of mounting tensions.

The reference sources that have informed the main orientations of this document are:

- Recommendation of the Council of the European Union of 23 May 2024 (Council of the EU, 2024);
- National Model for Research Integrity and Security and Guidelines for Research Institutions, issued by the Ministry of University and Research (MUR, 2024);
- European Charter for Researchers (Council of the European Union, 2023b).

Situated within the framework of European policies and responding to the national guidance *currently available*, this document outlines general principles and some operational measures compatible with the specific characteristics of a University primarily oriented towards the social sciences and humanities (SSH).

The University of Macerata has already adopted a Code of Ethics (Rector's Decree No. 254 of 7 July 2012), a Code of Conduct for University Staff (Rector's Decree No. 317 of 4 August 2015), and a Research Ethics Committee (Regulation issued by Rector's Decree No. 361 of 30 October 2020) working to ensure that research complies with the ethical principles of national, European and international regulations. The University also has a Regulation on the assignment of collaboration contracts to third parties (revised by Rector's Decree No. 99 of 26 February 2025), which governs the requirements and procedures for awarding individual assignments, through self-employment contracts, to persons external to the University.

The Codes and Regulations mentioned here remain valid with regard to ethics, integrity, personal data protection, conflicts of interest and transparency. This policy does not replace them; its purpose is to provide a framework that includes and further develops issues relating to research security. At this stage, since MUR has yet to release the national self-assessment tools — the risk-assessment matrix individual researchers will be required to complete — the University adopts a gradual and proportionate approach, focused primarily on raising awareness, building skills and strengthening institutional capacity. The more detailed definition of the procedures to be adopted for risk assessment and mitigation is deferred to a later stage, pending further guidance and tools from MUR.

Definitions

For the purposes of this document, the following definitions apply.

- **Research Security**. As indicated in the National Model (MUR, 2024) and in the Recommendation of the Council of the European Union (2024), research security refers to anticipating and managing risks relating to:

  a) the undesired transfer of critical knowledge and technologies that may compromise the security of the Union and its Member States, for example if diverted towards military or intelligence uses in third countries;

  b) malicious interference in research, which may result in its instrumentalisation by third countries for purposes including, among others, creating disinformation or encouraging self-censorship among

students and researchers, thereby violating academic freedom and the integrity of research within the Union;

c) violations of ethics or integrity, in which knowledge and technologies are used to repress, violate or undermine the Union's fundamental values and rights as defined in the Treaties.

- **Integrity of research and researchers**. Adherence to the professional values, principles and best practices that guarantee and uphold the validity, social relevance, accountability and quality of research (SIGRE, 2024; MUR, 2024).
- **Freedom of research**. Freedom of scientific research is closely linked to freedom of expression, freedom of association, freedom of movement, and the right to education, among other rights. It includes the right to freely define research questions, to choose and develop theories, to collect empirical data, and to adopt rigorous academic research methods, as well as to question established knowledge and propose new ideas. It also implies the right to openly share, disseminate and publish the related results, including through training and teaching activities. Freedom of scientific research includes researchers' right to express their opinions without suffering prejudice or disadvantage arising from the system in which they operate, or from governmental or institutional forms of censorship or discrimination. It also includes the freedom to join professional or representative academic bodies (Ministerial Conference, 2020).
- **Responsible internationalisation**. Responsible internationalisation means promoting international cooperation, mobility and knowledge sharing in an open and inclusive manner, while at the same time safeguarding research security, scientific integrity, academic freedom, intellectual property and the fundamental values of research. It implies the ability to identify, assess and manage the risks associated with international collaborations, while preserving the benefits deriving from openness and the global exchange of knowledge (Council of the European Union, 2023a).
- **External collaborations and external funding sources**. The National Model (MUR, 2024) defines the following types of collaboration and funding as external:
    - collaborations with parties/institutions outside the European Union, or not belonging to international institutions recognised through treaties (e.g. UN, CERN and WHO);
    - collaborations with parties not belonging to public institutions;
    - funding from institutions outside the European Union (e.g. research grants, including competitive ones, issued by non-EU public bodies), or not belonging to international institutions recognised through treaties (e.g. UN, CERN and WHO);
    - funding from private entities.

Parties Addressed by this Policy

This policy applies to research activities carried out at the University or under its responsibility, including project activities, international collaborations, data collection and processing, dissemination activities, scientific mobility, and visits by external staff. It is addressed to teaching and research staff, PhD students, research fellows, technical-administrative staff involved in research management and, where relevant, external collaborators.

Context

International cooperation, freedom of research and knowledge exchange are fundamental to scientific progress and innovation. In 2013, the European Commission identified the internationalisation of higher education institutions as a key driver of innovation, competitiveness and quality in higher education systems (European Commission, 2013). This approach was consolidated further in the following years through the promotion of the "three Os" paradigm (Open Science, Open Innovation and Open to the World), which placed research openness, international collaboration and the circulation of knowledge at the centre of European policy as key factors for scientific and economic progress (European Commission, 2015).

Following the COVID-19 pandemic, the issue of research security gained increasing prominence in European political debate. In 2021, the Council of the European Union promoted an approach to international cooperation summarised in the principle "as open as possible, as closed as necessary" (Council of the European Union, 2021). This issue has also attracted the attention of international organisations such as the OECD and the G7 SIGRE group (Security and Integrity of the Global Research Ecosystem), whose work seeks to strike a balance between openness and security, fostering an optimal collaborative environment.

A further significant step took place in 2024, with the publication of the Council of the EU Recommendation proposing strategies to protect critical technologies and safeguard academic freedom, while at the same time supporting forms of responsible internationalisation. The Recommendation invites Member States to develop national action plans and adequate governance mechanisms, identifying the undesired transfer of knowledge, foreign interference, and violations of research ethics and integrity among the main risks. Although not binding, it provides a reference framework for the actions of European institutions, Member States and the research community.

In Italy, MUR set up an ad hoc working group in 2024, which drafted a National Model and Guidelines for research security and integrity. MUR has also launched a dedicated website, already operational although some pages are still being completed (https://www.sicurezzaricerca.mur.gov.it/).

MUR envisages a Model structured on two levels:

- National level: a Centre for Research Security and Integrity, as suggested by the Council of the EU Recommendation, providing support, training and the definition of common procedures;
- Decentralised level: Research Security and Integrity Officers within universities, fostering the connection between the National Centre and the institutions themselves.

The MUR Guidelines identify a number of operational priorities for research institutions. At the organisational and cultural level, institutions are required to raise awareness among academic staff through appropriate communication tools and training programmes, and to adopt codes of conduct on conflicts of interest and transparency. In terms of risk assessment and management, institutions are called upon to establish preliminary self-assessment processes to identify the critical issues associated with research activities, to assess the risks posed by collaborations, grants, contracts and donations from external parties, and to put in place security measures for international travel and visits by external staff. Finally, specific guidance addresses the technologies and data most exposed to risk: on the one hand, data protection and cybersecurity, to be ensured through risk-analysis tools and mitigation measures in compliance with the European NIS-2 Directive; on the other, the management and mitigation of risks linked to dual-use goods and technologies (which can be used for both civil and military applications), in compliance with current EU and national legislation.

The preliminary self-assessment process will be based on a form that MUR will make available to estimate the critical issues associated with the activities to be undertaken. As a general rule, if the collaboration does not involve external partners and/or external funding (as defined in the MUR "National Model" document referred to above), it will be sufficient to declare this. Otherwise, the person responsible will carry out an analysis according to three possible categories of related critical issues: a) the scientific or technological field in which the activity is situated; b) the persons and institutions with which the collaboration takes place; and c) the entities funding the activities.

Research Security and Integrity: The SSH Disciplines

The social sciences and humanities (SSH) are not generally associated with the production of technologies with dual-use potential. However, they are not exempt from risks related to research security. Research activities in the SSH field may involve the collection and analysis of sensitive data, the involvement of vulnerable communities, and the production of knowledge susceptible to improper or instrumental use. Furthermore, international collaborations and dissemination activities may expose researchers to forms of undue interference or to pressure aimed at influencing scientific priorities.

Recent European initiatives on research security highlight the cross-cutting nature of these risks. They specify that the protection of scientific integrity, academic freedom and the responsible management of data and collaborations concern the entire research system, regardless of disciplinary sector (European Commission, 2024; OECD, 2022). In this context, promoting a culture of research security within SSH disciplines also means strengthening ethical responsibility, protecting research participants, and ensuring that openness and international cooperation develop in an informed and responsible manner, in line with the principles of responsible internationalisation promoted at European level (Council of the European Union, 2021).

Table 1 illustrates some examples of risks relevant to SSH disciplines, as mentioned in the reference sources.

Table 1. Possible risks for SSH disciplines

Risk area	Concrete examples in SSH disciplines	Possible consequences	Reference sources
Management of **special categories of personal data**	Collection and analysis of personal data or data belonging to special categories (e.g. political opinions, religious beliefs, ethnic affiliation, social or cultural orientation); management of interviews or archives containing identifiable information.	Privacy breaches; misuse of data; harm to participants; legal and reputational liability.	European Commission, 2024; OECD, 2022; GDPR (Regulation EU 2016/679)
Involvement of **vulnerable communities**	Research on migrants, refugees, minorities, marginalised communities or groups exposed to political or social risks.	Risks to participants' safety or wellbeing; exposure to retaliation or stigmatisation.	European Commission, 2021
Undue **interference** or external **pressure**	Attempts to influence research topics, the interpretation of results, or their dissemination, especially in international or politically sensitive contexts.	Compromised scientific independence; self-censorship; loss of scientific integrity.	Council of the European Union, 2021; European Commission, 2024

Risk area	Concrete examples in SSH disciplines	Possible consequences	Reference sources
High-risk international collaborations	Partnerships with institutions or entities located in geopolitically sensitive contexts or characterised by restrictions on academic freedom.	Undesired transfer of knowledge; misuse of results; reputational or legal risks.	European Commission, 2024; OECD, 2022
Misuse or **instrumentalisation of results**	Research results used for propaganda, discriminatory or social-manipulation purposes.	Distortion of scientific meaning; social or reputational harm; loss of public trust in research.	European Commission, 2024; OECD, 2022
Management and preservation of **sensitive archives and materials**	Digitisation or dissemination of historical archives, oral testimonies, or culturally sensitive materials.	Unauthorised access; misuse or decontextualisation of materials.	OECD, 2022; ALLEA, 2023
Protection of research **integrity and ethics**	Pressure to alter results or omit relevant information; collaboration with partners who do not meet equivalent ethical standards.	Violations of scientific integrity; loss of institutional credibility.	ALLEA, 2023; European Commission, 2024
Risks related to communication and **dissemination**	Public dissemination of sensitive results via media or social networks; misuse of information by third parties.	Manipulation of information; exposure to disinformation campaigns.	European Commission, 2023 (Defence of Democracy); OECD, 2022
Psychological and physical **safety** of research participants	Research activities in dangerous locations or on sensitive topics (e.g. gender-based violence, crime, repressive political regimes).	Exposure to retaliation, secondary psychological trauma, or threats to personal safety in the field.	European Commission, 2021

Building a culture of research security and integrity (2026-2029)

Pending the full definition of the national risk self-assessment tools and the operational guidance envisaged at ministerial level, the University adopts a gradual and proportionate approach to facilitate the development of a shared culture of research security and integrity.

The measures set out in this section do not, at this stage, introduce generalised procedures or additional administrative obligations; rather, they aim to support researchers in consciously identifying potentially sensitive situations, promoting good practices and facilitating access to institutional forms of support.

In line with the principles of responsible internationalisation and freedom of research, the University is committed to ensuring that openness to international scientific cooperation remains a core value, supported by tools that foster awareness and responsibility appropriate to the disciplinary context, with particular attention to the distinctive features of the social sciences and humanities.

The measures outlined here are based on the principle of proportionality, according to which the intensity of the tools adopted must be commensurate with the nature of the research activities and the risks actually identifiable, avoiding generalised or excessively burdensome approaches. They will be integrated into the University's HRS4R strategy (Human Resources Strategy for Researchers – Excellence in Research).

1. Awareness-raising and Information

Objective: to strengthen awareness and provide information.

- development of an institutional information page on research security and integrity;
- organisation of seminars and workshops (online or in person), also aimed at PhD students;
- integration of the topic of research security into existing training activities on research ethics and data protection.

Responsibility: Vice-Rector and Delegates for Research; Research and Innovation Area; for dissemination activities: Communications Office; Doctoral School; Training Programmes Operational Unit.

2. Support and Advice

Objective: to provide a point of reference.

- appointment of an institutional Research Security Advisor (within the Research and Innovation Area) to provide advice and support, and to promote informed and proportionate risk management by suggesting mitigation measures
- creation of an advisory channel to be consulted in case of doubts concerning:
    - international collaborations;
    - management of special categories of personal data;
    - involvement of external partners;
- periodic meetings to strengthen coordination between:
    - the Research and Innovation Area;
    - the DPO (Data Protection Officer);
    - the Ethics Committee;
    - the Doctoral School;
    - the Internationalisation and ERUA Area;
- preparation of a handbook (Vademecum) for international travel and visits by external staff.

Responsibility: Vice-Rector and Delegates for Research; Vice-Rector and Delegates for Internationalisation; Internationalisation and ERUA Area; Research and Innovation Area.

3. Promotion of Good Practice in Research Management

Objective: to guide behaviour.

- preparation of concise operational recommendations encouraging staff to:
    - pay attention to the nature of the data collected, and to its management and storage;

- verify the transparency of external partners;
- clearly define the conditions for the publication of results;
- ensure adequate protection of research participants;
- carefully assess the public dissemination of sensitive results;
- promote the use of clear agreements with external partners, especially regarding:
  - data access;
  - data management;
  - use of results;
  - intellectual property.

Responsibility: Vice-Rector and Delegates for Research; Research and Innovation Area; Data Steward and Research Security Advisor.

4. Gradual Approach to Developing Self-Assessment Tools

The University is committed to developing, at a later stage, risk self-assessment tools consistent with national guidance and with the future operational guidelines issued by MUR. Any introduction of such tools will continue to be guided by the principle of proportionality, avoiding unnecessary burdens and ensuring full compatibility with the University's disciplinary specificities.

As regards the risks that the use of Artificial Intelligence systems may entail, reference is made to the general principles already formulated by the University, and to the specific guidelines on the use of AI tools in research, which are currently being drafted. In terms of cybersecurity, the University has already taken the necessary steps to comply with the European NIS-2 Directive, transposed into Italian law by Legislative Decree No. 138 of 4 September 2024.

5. Monitoring and Progressive Updating

The University promotes continuous monitoring of the evolution of the national and European regulatory framework on research security. The measures set out in this policy will be subject to periodic review, in particular following the publication of further operational guidance by the competent national authorities.

References

ALLEA (2023), European Code of Conduct for Research Integrity – Revised Edition (https://allea.org/wp-content/uploads/2023/06/European-Code-of-Conduct-Revised-Edition-2023.pdf)

Council of the European Union (2021), Council Conclusions on the Global Approach to Research and Innovation – Europe's Strategy for International Cooperation in a Changing World (https://data.consilium.europa.eu/doc/document/ST-12301-2021-INIT/en/pdf)

Council of the European Union (2023a), Knowledge Security and Responsible Internationalisation (https://data.consilium.europa.eu/doc/document/ST-12301-2021-INIT/en/pdf)

Council of the European Union (2023b), Council Recommendation on a European Framework to Attract and Retain Research, Innovation and Entrepreneurial Talents in Europe – Annex II: European Charter for Researchers (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202301640)

Council of the European Union (2024), Council Recommendation on Enhancing Research Security (https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf)

European Commission (2013), European Higher Education in the World (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1402397801375&uri=CELEX:52013DC0499)

European Commission (2015), Open Science, Open Innovation, Open to the World – A Vision for Europe, DG Research & Innovation (https://op.europa.eu/en/publication-detail/-/publication/3213b335-1cbc-11e6-ba9a-01aa75ed71a1)

European Commission (2021), Ethics in Social Science and Humanities (https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-in-social-science-and-humanities_he_en.pdf)

European Commission (2023), Communication on Defence of Democracy (https://commission.europa.eu/publications/documents-defence-democracy_en)

European Commission (2024), Proposal for a Council Recommendation on Enhancing Research Security (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0026)

Ministerial Conference on the European Research Area (2020), Bonn Declaration on Freedom of Scientific Research (https://www.bmftr.bund.de/SharedDocs/Downloads/EN/b/bonn_declaration_en.pdf?__blob=publicationFile&v=5)

MUR (2024), National Model for the Integrity and Security of Research (https://www.sicurezzaricerca.mur.gov.it/wp-content/uploads/2025/08/Modello-Nazionale.pdf)

OECD (2022), Integrity and Security in the Global Research Ecosystem (https://www.oecd.org/en/publications/2022/06/integrity-and-security-in-the-global-research-ecosystem_2bd8511d.html)

SIGRE (2024), G7 Best Practices for Secure and Open Research (https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-best-practices-secure-and-open-research)