

STUDIES-DIG

Project 101131544 - HORIZON-MSCA-2022-SE-01

Models and Instruments for Transforming Higher Education Systems through Transnational Multi-Sector Links

Secondment Report

Work Package 3 - Identifying and mapping digital risks, threats and their impact on social skills

Contributions to Tasks 3.1, 3.4 and 3.5

Seconded researcher	Helena Belchior Rocha, Assistant Professor
Sending institution	Iscte – Instituto Universitário de Lisboa, Portugal
Receiving institution	NORVAGE, Türkiye
Secondment period	4 August 2026 – 12 September 2026 (30 days)
Sending institution contact	Professor David Ferraz
Date of report	29/09/2026

Contents

1. Executive summary	3
2. Secondment details and objectives	3
2.1 Administrative information	3
2.2 Objectives of the secondment	4
3. Activities carried out	4
3.1 Research work plan	4
3.2 Working meetings and scientific exchange	5
3.3 Methodological exchange	5
4. Scientific outputs	5
4.1 Task 3.1 - Literature review and desk research on digital risks and threats	6
4.2 Task 3.4 - Comparative mapping framework of digital risks	8
4.3 Task 3.5 - Digital risks and social skills: conceptual and empirical analysis .	10
5. Publications and dissemination	11
6. Contribution to the project, impact and next steps	12
6.1 Contribution to WP3 tasks	12
6.2 Added value and impact	12
6.3 Next steps	13
7. Conclusion	13
References	14

1. Executive summary

This report documents the secondment of Helena Belchior Rocha (Iscte - Instituto Universitário de Lisboa) to NORVAGE in Türkiye, carried out between 4 August and 12 September 2026 under the MSCA Staff Exchanges project STUDIES-DIG (Grant Agreement 101131544). The secondment was implemented within Work Package 3, which is dedicated to identifying and mapping digital risks and threats and their impact on social skills, and was designed to contribute directly to Task 3.1 (desk research), Task 3.4 (mapping of digital risks and threats) and Task 3.5 (analysis of the relationship between digital risk and social skills).

During the secondment the researcher conducted an extended literature review and desk research on digital risks across sectors, developed a comparative mapping framework that can be applied across organizational and national contexts, and advanced a conceptual and empirical analysis of how social skills operate as protective factors against digital risk. The work was discussed and refined in working meetings with Professor Ömer Delialioğlu of the Middle East Technical University (METU), Ankara, and with Iscte colleague Tiago Lapa, in which the first outputs of the secondment were reviewed and the next steps for joint research were agreed.

The secondment produced two scientific articles, both now submitted to peer-reviewed journals and awaiting review. First, *Who Is at Risk? How Academic Staff Judge Students, Colleagues and Themselves on Artificial Intelligence in Higher Education*, examines how academic staff perceive the distribution of AI-related risk across different groups in the university. The second, *Supporting the AI Transition in Higher Education: How Institutions Can Equip Teaching Staff and Students*, Evidence from a Six-Country Staff Survey draws on comparative survey evidence to identify the institutional supports that staff consider necessary for a responsible transition to AI. Both articles are co-authored with colleagues from the STUDIES-DIG consortium, including Professor David Ferraz, and constitute direct outputs of WP3. Together with the literature review and the mapping framework presented in this report, they fulfil the scientific outcomes foreseen in the secondment agreement.

2. Secondment details and objectives

2.1 Administrative information

Project	STUDIES-DIG — Models and Instruments for Transforming Higher Education Systems through Transnational Multi-Sector Links (101131544, HORIZON-MSCA-2022-SE-01)
Participant	Helena Belchior Rocha, Assistant Professor,

Sending institution	Iscte – Instituto Universitário de Lisboa, Av. das Forças Armadas, 1649-026 Lisboa, Portugal
Receiving institution	NORVAGE, Türkiye
Period	4 August 2026 - 12 September 2026; 30 days of secondment activity, plus one travel day before the start of the activity
Work Package	WP3 - Identifying and mapping digital risks, threats and their impact on social skills
Tasks addressed	Primary: Tasks 3.1, 3.4 and 3.5. Supporting contributions to Tasks 3.2 and 3.3

2.2 Objectives of the secondment

The overall objective of the secondment was to strengthen interdisciplinary and cross-sectoral research collaboration between Iscte and the receiving partner within STUDIES-DIG. The secondment agreement specified five concrete aims: to conduct comparative desk research on digital risks and threats affecting employees, business organizations, governmental and non-governmental organizations, higher education institutions, trainers and academic administrative staff; to develop a systematic mapping of digital risks across institutional and national contexts, identifying typologies, vulnerabilities and sector-specific dynamics; to analyze the relationship between digital risks and social skills, with emphasis on critical thinking, emotional regulation, collaboration and digital literacy; to promote methodological exchange and harmonization of research tools between partners; and to build capacity in the analysis of socio-digital transformations in organizational and educational settings.

The expected scientific outcomes were a comprehensive literature review and desk research report (Task 3.1), a comparative mapping framework of digital risks (Task 3.4), a conceptual and empirical analysis of the relationship between digital risks and social skills leading to co-authored publications (Task 3.5), and contributions to peer-reviewed articles, conference presentations and joint research outputs. Section 4 reports on each of these in turn.

3. Activities carried out

3.1 Research work plan

The secondment was organized in three overlapping phases. The first phase was devoted to desk research: identifying, screening and synthesizing academic literature, policy documents and institutional reports on digital risks across sectors, with particular attention to higher education and to the growing body of

work on generative artificial intelligence. The second phase focused on analytical synthesis, translating the reviewed literature into a structured typology of digital risks and a comparative mapping framework that accounts for stakeholder group, organizational setting and national context. The third phase concentrated on the relationship between digital risks and social skills, on the analysis of comparative survey data from academic staff, and on drafting the two scientific articles that resulted from the secondment.

3.2 Working meetings and scientific exchange

Meeting with Professor Ömer Delialioglu, Middle East Technical University (METU), Ankara. The meeting was used to present and discuss the first outputs of the secondment, namely the preliminary structure of the literature review, the draft risk typology and the initial analyses of the staff survey. The discussion addressed how digital risks and institutional responses to AI differ between the Portuguese and Turkish higher education systems, how national regulatory frameworks shape institutional preparedness, and how the mapping framework could be applied to Turkish institutions. The exchange provided a valuable external perspective on the comparative dimension of Task 3.4 and identified opportunities for further joint work between the partners.

Meeting with Tiago Lapa, Iscte -This working meeting reviewed the first outputs of the secondment with a focus on the conceptual framing of digital risk and social skills (Task 3.5) and on the analytical strategy for the two articles. The discussion drew on Iscte's expertise in digital inclusion and online risk research and helped to connect the higher education focus of the secondment with broader research on digital skills, digital inequalities and the classification of online risks. Decisions were taken on the structure and target journals of the two manuscripts.

3.3 Methodological exchange

In line with the secondment objectives, the researcher contributed to the methodological exchange between partners, with emphasis on qualitative and mixed methods approaches to the study of digital risk. This included discussion of how survey instruments on digital risk perception and AI use can be harmonized across countries, how closed and open-ended items can be combined to capture both the prevalence and the meaning of perceived risks, and how the resulting data can be linked to the mapping framework. These exchanges also informed the preparation of survey questions under Task 3.2 and the fieldwork planned under Task 3.3.

4. Scientific outputs

4.1 Task 3.1 - Literature review and desk research on digital risks and threats

Scope and approach

The desk research covered academic literature, European and international policy frameworks, and institutional and agency reports. Sources were selected for their relevance to the stakeholder groups named in the secondment agreement: employees and business organizations, governmental and non-governmental organizations, higher education institutions, lecturers and trainers, and administrative staff in the academic sector. The review was organized thematically rather than by discipline, because digital risks are studied in fields as different as information security, media and communication studies, organizational psychology, education and law, and each field tends to capture only part of the phenomenon.

Conceptualizing digital risk

The first finding of the review is that the concept of digital risk is used in two distinct senses. In technical and organizational literature, digital risk refers mainly to threats to information systems and data, such as malware, ransomware, phishing and data breaches, which are documented annually in sources such as the ENISA Threat Landscape (ENISA, 2024). In the social science literature, the concept extends to the harms that people experience through digital environments, including harmful content, harmful contact, problematic conduct and exploitative commercial practices; the 4Cs classification developed for online risks to children (Livingstone & Stoilova, 2021) is a widely used example that can be adapted to adult and institutional settings. A useful working definition for WP3 therefore combines both traditions: digital risks are the potential for harm to individuals, organizations or societies that arise from the use, design or governance of digital technologies. Importantly, literature consistently distinguishes risk from harm: exposure to a risk does not automatically lead to harm, and the outcome depends on individual skills, social support and institutional conditions.

Main risk domains across sectors

Cybersecurity and data protection. Across all sectors, the human factor remains central to security incidents. Research on risky cybersecurity behaviour shows that attitudes, impulsivity and habits of use predict vulnerability to threats such as phishing (Hadlington, 2017). Universities are particularly exposed because they combine open network cultures, large and rotating user populations and valuable research data. In the European context, the General Data Protection Regulation (Regulation (EU) 2016/679) defines the obligations of institutions; in Türkiye, the Law on the Protection of Personal Data (Law No. 6698, 2016) plays a comparable role, which makes data protection a natural axis of comparison between the two partner contexts.

Information disorder. Misinformation, disinformation and malformation affect citizens, organizations and public authorities alike (Wardle & Derakhshan, 2017). For higher education, the risk is twofold: students and staff are exposed to false information, and universities carry a particular responsibility for cultivating the critical judgement that protects against it.

Relational and interpersonal risks. Cyberbullying, online harassment and hostile online interaction have been extensively documented among young people (Smith et al., 2008) and are increasingly recognized in workplaces and universities, including harassment of academics in public online debate. These risks are closely related to the social skills addressed in Task 3.5.

Wellbeing and technostress. Digitalization of work has created new sources of strain, including information overload, constant connectivity, and the pressure to adapt continually to new tools. Technostress literature shows that such conditions increase role stress and can reduce productivity (Tarafdar et al., 2007). Lecturers, trainers and administrative staff have been especially affected by the rapid expansion of digital teaching and administration.

Digital exclusion and inequality. Research on digital inequalities shows that access alone does not determine outcomes; differences in skills, uses and social resources shape who benefits from digital technologies and who is harmed by them (van Deursen et al., 2016; Helsper, 2021). Digital risk is therefore unequally distributed across social groups, organizations and countries.

Risks associated with artificial intelligence. The fastest-growing strand of literature concerns artificial intelligence, and generative AI. In higher education, the main concerns identified are threats to academic integrity and assessment (Cotton et al., 2024), over-reliance and the erosion of learning and professional skills, bias and opacity of algorithmic systems, privacy and data governance, and the unequal preparedness of staff and students (Kasneci et al., 2023). Earlier reviews had already noted that research on AI in higher education paid limited attention to educators themselves (Zawacki-Richter et al., 2019), a gap that the two articles produced during this secondment address directly. Policy guidance has developed rapidly, including UNESCO's guidance on generative AI in education and research (UNESCO, 2023) and the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), which classifies certain uses of AI in education as high-risk.

State of the art and research gaps

The review identified four gaps that are relevant to the STUDIES-DIG project. 1- digital risks are usually studied within single sectors and single disciplines, which makes cross-sector comparison difficult and justifies the integrated mapping developed under Task 3.4. 2- most studies measure exposure to risk rather than the conditions that transform risk into harm or into resilience. 3- the role of social and socio-emotional skills as protective factors is often assumed but rarely tested,

particularly among adults and professionals. 4- comparative evidence on how academic staff perceive and respond to AI-related risks across countries remains scarce, especially evidence that includes countries outside Western Europe. These gaps structured the subsequent work on the mapping framework and on the relationship between digital risks and social skills.

4.2 Task 3.4 - Comparative mapping framework of digital risks

Building on the desk research, a comparative mapping framework was developed to allow digital risks to be described and compared across stakeholder groups, organizational settings and national contexts. The framework is organized along three axes. The first axis is the risk domain, using the six domains identified in the literature review. The second axis is the level of analysis, distinguishing individual risks (experienced by a student, employee or lecturer), organizational risks (affecting an institution's operations, reputation or mission) and systemic risks (affecting a sector or a society). The third axis is the context, which captures the organizational and national conditions that shape both exposure to risk and the capacity to respond.

Table 1 presents the core of the framework: for each risk domain, it summarizes typical manifestations, the stakeholder groups most exposed according to the literature, and the social skills that are expected to act as protective factors. The last column provides the bridge between Task 3.4 and Task 3.5.

Risk domain	Typical manifestations	Most exposed stakeholders	Protective social skills
Cybersecurity and data protection	Phishing and social engineering; ransomware; data breaches; misuse of personal and research data	Administrative staff; employees in SMEs and public bodies; HEIs holding sensitive data	Critical thinking; digital literacy; cooperation and reporting behaviour
Information disorder	Misinformation and disinformation; manipulated content; erosion of trust in expertise	Students; general public; NGOs and public authorities	Critical thinking; source evaluation; perspective-taking
Relational and interpersonal	Cyberbullying; online harassment; hostile interaction; reputational attacks	Students; early-career staff; academics active in public debate	Empathy; emotional regulation; communication; help-seeking
Wellbeing and technostress	Information overload; constant connectivity; blurred work-life boundaries	Lecturers and trainers; administrative staff; employees in digitalised workplaces	Emotional regulation; self-management; collaboration

Risk domain	Typical manifestations	Most exposed stakeholders	Protective social skills
Digital exclusion and inequality	Unequal access, skills and support; exclusion from digital services and learning	Older and less qualified workers; disadvantaged students; smaller organisations	Digital literacy; peer support; collaborative learning
AI-related risks	Threats to academic integrity; over-reliance and deskilling; bias and opacity; privacy; unequal preparedness	Students; teaching staff; HEIs as institutions; employers	Critical thinking; ethical judgement; adaptability; collaboration

Table 1. Core matrix of the comparative mapping framework: risk domains, exposure and protective social skills.

The contextual axis is operationalized through a set of comparative dimensions that can be applied to any organization or country. These dimensions, presented in Table 2, allow the same risk to be interpreted differently depending on the regulatory, institutional and cultural environment in which it arises. For example, the risks associated with generative AI in a university depend not only on the technology itself but on whether the institution has a policy on AI use, whether staff have received training, and how national regulation frames the use of AI and personal data.

Contextual dimension	Guiding questions for mapping	Indicative sources and indicators
Regulatory environment	Which legal frameworks govern data protection, cybersecurity and AI, and how binding are they for the organization?	GDPR and EU AI Act (Portugal); Law No. 6698 on Personal Data Protection (Türkiye); sectoral regulation
National digital maturity	What is the level of digital infrastructure, skills and cybersecurity capacity in the country?	European Commission Digital Decade Indicators; ITU Global Cybersecurity Index; OECD skills data
Organizational digital maturity	Does the organization have digital strategies, policies, dedicated staff and incident procedures?	Institutional documents; interviews; survey items developed under Task 3.2
Institutional support and training	What training and guidance are available for staff, students and administrators?	Staff survey data; DigComp and DigCompEdu frameworks as benchmarks
Organizational culture	Is there a culture of openness, collaboration and reporting around digital incidents and innovation?	Qualitative interviews; open-ended survey responses
Stakeholder composition	Which groups are present, and how do their roles shape exposure to risk?	Mapping of target groups used in Task 3.3

Table 2. Contextual dimensions for comparing digital risks across organizations and countries.

The framework is designed to be used in three ways within STUDIES-DIG: as a coding structure for the desk research and for qualitative material collected by partners; as a reference for the design and interpretation of the electronic surveys under Tasks 3.2 and 3.3; and as a template for comparative country and sector profiles, starting with the Portuguese and Turkish contexts represented in this secondment. Its application to empirical data from the consortium is proposed as a next step (Section 6).

4.3 Task 3.5 - Digital risks and social skills: conceptual and empirical analysis

Conceptual model

The conceptual analysis starts from the distinction, established in the literature review, between exposure to digital risk and the experience of harm. The proposed model positions social skills as the key resources that shape whether exposure leads to harm or to resilience. Four groups of skills are distinguished, following the secondment agreement and the European competence frameworks DigComp 2.2 (Vuorikari et al., 2022) and DigCompEdu (Redecker, 2017).

Critical thinking enables people to evaluate information and sources, recognize manipulation and make reasoned judgements about when and how to use digital tools, including AI (Facione, 1990). Emotional regulation allows individuals to manage the stress, anxiety and impulsive reactions that digital environments can trigger, which is relevant both to wellbeing risks and to security risks that exploit urgency or fear (Gross, 1998). Collaboration and communication support help-seeking, the sharing of knowledge about threats and the collective development of good practice within teams and institutions. Digital literacy, understood broadly to include operational, informational, social and creative skills (van Deursen et al., 2016), provides the technical and informational basis on which the other skills operate.

The model proposes three types of relationship. Social skills may act as protective factors that reduce the likelihood that exposure results in harm; as moderators that weaken the link between risk exposure and negative outcomes; and as outcomes in their own right, since some digital risks, such as over-reliance on AI or technostress, may erode the very skills that protect against them. This last relationship is particularly important for higher education, whose mission includes developing the critical and social competences that students need in digital societies. The model also highlights that individual skills are embedded in institutional conditions: skills are more likely to translate into resilience when institutions provide clear guidance, training and a supportive culture.

Empirical analysis

The empirical component of Task 3.5 focused on artificial intelligence as the most rapidly evolving area of digital risk in higher education. It draws on a comparative survey of academic staff conducted in six countries, which captured how staff perceive AI-related risks, how they judge the preparedness and vulnerability of different groups, and what institutional support they consider necessary.

The analysis addressed two questions that link directly to the conceptual model. The first concerns the perceived distribution of risk: whom academic staff see as most at risk from AI, and do they judge students, colleagues and themselves differently? This question speaks to the literature on the third-person effect, which shows that people tend to perceive others as more vulnerable to media influence than themselves (Davison, 1983) and has implications for how institutions target training and support. The second concerns institutional support: what resources, policies and forms of training do staff consider necessary to equip both teaching staff and students for the AI transition, and how do these needs vary across national contexts?

Taken together, the conceptual model and the empirical analysis support a central argument of WP3: that responses to digital risk in higher education cannot rely on technical solutions or rules alone, but must also invest in the critical, emotional and collaborative skills of staff and students, supported by coherent institutional strategies.

5. Publications and dissemination

The secondment led to two scientific articles, both submitted to peer-reviewed journals and currently awaiting review. They are co-authored with colleagues from the STUDIES-DIG consortium, including Professor David Ferraz (Iscte), and will acknowledge the funding of the project under the MSCA Staff Exchanges programme. Both articles contribute to Task 3.5 and draw on the literature review and mapping work of Tasks 3.1 and 3.4.

#	Article	Authors and status
1	Who Is at Risk? How Academic Staff Judge Students, Colleagues and Themselves on Artificial Intelligence in Higher Education Examine how academic staff assess the exposure of students, colleagues and themselves to AI-related risks, and what these judgements imply for institutional support strategies.	Helena Belchior Rocha, and David Ferraz Journal: Journal of Management Education (JME) Status: To be submitted in october

#	Article	Authors and status
2	Supporting the AI Transition in Higher Education: How Institutions Can Equip Teaching Staff and Students - Evidence from a Six-Country Staff Survey Draws on comparative survey evidence from academic staff in six countries to identify the institutional support needed for a responsible transition to AI in teaching and learning.	Helena Belchior Rocha, Omer Delialioglu David Ferraz and Tiago Lapa Journal: Education and Information Technologies Status: submitted, awaiting review

Table 3. Scientific articles resulting from the secondment.

Once accepted, the articles will be published in open access in line with Horizon Europe requirements and deposited in Iscte's institutional repository. Both articles will be proposed for presentation at relevant international conferences and at STUDIES-DIG consortium meetings. The literature review and mapping framework presented in this report are also available as input for the WP3 deliverables and for further joint publications, including a possible comparative paper with METU colleagues.

6. Contribution to the project, impact and next steps

6.1 Contribution to WP3 tasks

Task	Contribution of the secondment
Task 3.1	Thematic literature review and state of the art on digital risks across sectors, including a working definition of digital risk and identification of four research gaps (Section 4.1).
Task 3.2	Identification of potential factors of digital risk in academic and non-academic institutions; input to the design of survey questions through the contextual dimensions of the mapping framework.
Task 3.3	Methodological exchange on the harmonisation of survey instruments across countries and target groups.
Task 3.4	Comparative mapping framework combining risk domains, levels of analysis and contextual dimensions (Section 4.2).
Task 3.5	Conceptual model of digital risks and social skills and empirical analysis of AI-related risk in higher education, resulting in two submitted co-authored articles (Sections 4.3 and 5).

6.2 Added value and impact

For the institutions involved, the secondment enabled knowledge transfer on digital risk analysis and socio-technical systems, and it reinforced collaboration between Iscte, NORVAGE and METU. The comparison between the Portuguese and Turkish contexts added depth to the analysis and strengthened the external validity of the framework. For the project, the secondment delivered a shared analytical tool for WP3, an enriched empirical base and two publications that make the work of STUDIES-DIG visible to the international research community. At the societal level, the work supports evidence-based recommendations for strengthening social skills as protective factors against digital threats, and contributes to European debates on digital transformation and AI in higher education.

For the researcher, the secondment provided advanced experience in digital risk analysis and comparative research on AI in higher education, strengthened intercultural and interdisciplinary competences through work in a different national and institutional context, expanded her international network, particularly with colleagues in Türkiye, and contributed to career development through the preparation of two peer-reviewed publications.

6.3 Next steps

The following actions are planned to consolidate the results of the secondment:

- Follow the review process of the two submitted articles and revise them in response to reviewers' comments.
- Apply the mapping framework to empirical data collected by consortium partners under Tasks 3.2 and 3.3 and produce comparative profiles for the Portuguese and Turkish contexts.
- Develop the conceptual model of digital risks and social skills into a further co-authored publication, possibly in collaboration with METU.
- Present the results at consortium meetings and at international conferences and feed them into the WP3 deliverables and policy recommendations.

7. Conclusion

The secondment to NORVAGE achieved the objectives set out in the secondment agreement. It produced a literature review and state of the art on digital risks across sectors (Task 3.1), a comparative mapping framework applicable to different organizational and national contexts (Task 3.4), and a conceptual and empirical analysis of the relationship between digital risks and social skills (Task 3.5), which has already resulted in two co-authored articles submitted to peer-reviewed journals. The working meetings with Professor Ömer Delialioğlu (METU) and Tiago Lapa (Iscte) were essential for discussing the first outputs and

for shaping the next stages of joint research. The results provide a solid basis for the continuation of WP3 and for the long-term collaboration between the institutions involved.

References

- Cotton, D. R. E., Cotton, P. A., & Shipway, J. R. (2024). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International*, 61(2), 228–239.
- Davison, W. P. (1983). The third-person effect in communication. *Public Opinion Quarterly*, 47(1), 1–15.
- ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union*, L 119.
- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
- Facione, P. A. (1990). *Critical thinking: A statement of expert consensus for purposes of educational assessment and instruction*. American Philosophical Association.
- Gross, J. J. (1998). The emerging field of emotion regulation: An integrative review. *Review of General Psychology*, 2(3), 271–299.
- Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.
- Helsper, E. J. (2021). *The digital disconnect: The social causes and consequences of digital inequalities*. Sage.
- Kasneci, E., Seßler, K., Küchemann, S., et al. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, 102274.
- Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying online risk to children*. CO:RE Short Report Series on Key Topics. Leibniz-Institut für Medienforschung | Hans-Bredow-Institut.
- Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union.
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376–385.
- Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress on role stress and productivity. *Journal of Management Information Systems*, 24(1), 301–328.
- Türkiye. (2016). *Law No. 6698 on the Protection of Personal Data*. Official Gazette No. 29677.

- UNESCO. (2023). *Guidance for generative AI in education and research*. UNESCO.
- van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2016). Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society*, 19(6), 804–823.
- Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. Publications Office of the European Union.
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe.
- Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education*, 16, 39.

Project participant

Name: Helena Belchior Rocha

Signature:

Date: 29/09/2026

