

EDU-SECure

Cyber-Sicherheit und Empowerment vulnerabler Gruppen in Bildungseinrichtungen durch Prävention und digitale Tools

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS CS F&E-Dienstleistungen (CS FED_2025)	Status	laufend
Projektstart	01.11.2026	Projektende	31.10.2028
Zeitraum	2026 - 2028	Projektlaufzeit	24 Monate
Barwert der Projektförderung	€ 198.352		
Keywords	Cyber-Sicherheit im Bildungssektor; KI-basierte Gewaltformen; Cyber-Resilienz; Intersektionale Risikoanalyse; Geschlechtersensible Prävention		

Projektbeschreibung

Ausgangssituation, Problematik und Motivation: Die zunehmende Digitalisierung des Bildungsbereichs führt zu neuen Formen digitaler Gewalt, darunter Cybermobbing, bildbasierte Gewalt (z. B. Non-Consensual Intimate Images), Hate Speech sowie KI-gestützte Manipulationen wie Deepfakes oder algorithmisch verstärkte Stereotype. Diese Entwicklungen betreffen insbesondere Mädchen und junge Frauen sowie intersektional benachteiligte Schüler:innen.

Während digitale Grundbildung und Cyber-Sicherheit im Schulkontext zunehmend thematisiert werden, werden KI-basierte Gewaltformen bislang nur punktuell berücksichtigt und selten systematisch in pädagogische Unterstützungsangebote integriert. Lehrkräfte und Jugendliche stehen vor der Herausforderung, komplexe oder ambivalente Konstellationen wie etwa Grenzfälle zwischen Gruppendynamik, „Scherzen“ und gezielter digitaler Herabwürdigung einzuordnen und angemessen darauf zu reagieren. Es fehlt an empirisch fundierten, praxisnahen Instrumenten, die technische, soziale und gendersensible Perspektiven verbinden und Handlungssicherheit im schulischen Alltag fördern.

Ziele und Innovationsgehalt: EDU-SECure verfolgt das Ziel, digitale Gewalt im Bildungsbereich und insbesondere KI-basierte Risiken systematisch zu analysieren und darauf aufbauend niederschwellige, praxistaugliche Unterstützungsinstrumente zu entwickeln. Digitale Gewalt wird dabei als relevantes Cyber-Sicherheitsrisiko verstanden, das Prävention, Früherkennung und Reflexionsfähigkeit gleichermaßen betrifft.

Im Zentrum steht eine empirische Bedarfs- und Risikoanalyse, die aktuelle Erscheinungsformen digitaler Gewalt sowie spezifische Vulnerabilitäten im Bildungskontext untersucht. Auf dieser Grundlage wird ein strukturierter Risiko- und Szenarienkatalog entwickelt, der typische Konstellationen digitaler Gewalt systematisiert und mögliche Handlungsoptionen abbildet.

Die Innovation des Projekts liegt in der Verbindung von intersektionaler Analyse, partizipativer Entwicklung und szenarienbasierter Entscheidungslogik. Durch einen Co-Creation-Prozess mit Lehrkräften und Jugendlichen werden modulare Workshopkonzepte und Unterrichtsmaterialien entwickelt, die technisches Orientierungswissen zu KI und digitalen Risiken

mit sozialer Einordnung, gendersensibler Reflexion und konkreten Reaktionsmöglichkeiten verknüpfen („Mixed Skillset“). Ergänzend wird ein webbasiertes, interaktives Sensibilisierungs- und Unterstützungstool prototypisch umgesetzt, das ausgewählte Risikoszenarien in nachvollziehbare Entscheidungs- und Reflexionspfade übersetzt.

Angestrebte Ergebnisse und Erkenntnisse: Das Projekt generiert fundierte Erkenntnisse zu aktuellen Formen digitaler und KI-basierter Gewalt im schulischen Kontext sowie zu spezifischen Betroffenheitslagen vulnerabler Gruppen. Die Ergebnisse werden in einem Studienbericht und einem systematisierten Risiko- und Szenarienkatalog dokumentiert.

Darauf aufbauend entstehen erprobte Workshopkonzepte, Open Educational Resources sowie ein datenschutzkonformer Web-Prototyp eines szenarienbasierten Sensibilisierungs- und Unterstützungstools. Durch Pilotierung und qualitative Evaluation werden Praxistauglichkeit, Verständlichkeit und Reflexionspotenzial überprüft und weiterentwickelt.

EDU-SECure leistet damit einen evidenzbasierten Beitrag zur Stärkung der digitalen Resilienz junger Menschen und zur Unterstützung von Lehrkräften im Umgang mit digitalen und KI-basierten Gewaltformen im schulischen Alltag.

Abstract

Starting point, problem, and motivation: The increasing digitization of education is leading to new forms of digital violence, including cyberbullying, image-based violence (e.g., non-consensual intimate images), hate speech, and AI-supported manipulation such as deepfakes or algorithmically reinforced stereotypes. These developments particularly affect girls and young women, as well as intersectionally disadvantaged students.

While basic digital literacy and cyber security are increasingly being addressed in schools, AI-based forms of violence have so far only been considered sporadically and are rarely systematically integrated into educational support services. Teachers and young people face the challenge of classifying complex or ambivalent constellations, such as borderline cases between group dynamics, “joking,” and targeted digital degradation, and responding appropriately. There is a lack of empirically based, practical tools that combine technical, social, and gender-sensitive perspectives and promote confidence in everyday school life.

Objectives and innovative content: EDU-SECure aims to systematically analyze digital violence in education, particularly AI-based risks, and to develop low-threshold, practical support tools based on this analysis. Digital violence is understood as a relevant cyber security risk that affects prevention, early detection, and reflective capacity in equal measure.

The focus is on an empirical needs and risk analysis that examines current manifestations of digital violence and specific vulnerabilities in the educational context. On this basis, a structured risk and scenario catalog is being developed that systematizes typical constellations of digital violence and maps possible courses of action.

The innovation of the project lies in the combination of intersectional analysis, participatory development, and scenario-based decision-making logic. Through a co-creation process with teachers and young people, modular workshop concepts and teaching materials are developed that combine technical orientation knowledge about AI and digital risks with social classification, gender-sensitive reflection, and concrete response options (“mixed skill set”). In addition, a web-based, interactive awareness-raising and support tool is being prototyped that translates selected risk scenarios into comprehensible decision-making and reflection paths.

Desired results and findings: The project will generate sound findings on current forms of digital and AI-based violence in the school context and on specific situations affecting vulnerable groups. The results will be documented in a study report and a systematized risk and scenario catalog.

Based on this, proven workshop concepts, open educational resources, and a data protection-compliant web prototype of a scenario-based awareness and support tool will be developed. Through piloting and qualitative evaluation, practical suitability, comprehensibility, and reflection potential will be tested and further developed.

EDU-SECure thus makes an evidence-based contribution to strengthening the digital resilience of young people and supporting teachers in dealing with digital and AI-based forms of violence in everyday school life.

Projektkoordinator

- JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner

- Bundesministerium für Frauen, Wissenschaft und Forschung
- Österreichisches Institut für angewandte Telekommunikation