# ASCILITE 2026

***The Future is Connection:***

*Collaboration, Creativity and Compassion in a Digital Society*


# From academic integrity to digital exam wellbeing: Reframing secure exam infrastructure in the AI era


**Fernando Jativa**
University of Melbourne

**Filip Janic**
Schoolyear



Generative artificial intelligence has intensified pressure on universities to produce reliable evidence of student learning. This practice-informed conceptual paper introduces digital exam wellbeing as a framework for evaluating secure digital exam infrastructure for supervised, on-campus exams. Digital exam wellbeing describes a design objective: protecting assessment standards while limiting avoidable technical, cognitive, privacy and accessibility burdens, and supporting educator autonomy and operationally dependable delivery. The framework is developed through relevant literature and illustrated through a descriptive case of Schoolyear's Safe Exam Workspace, which supports approved websites, files, desktop applications and virtual desktops. The case illustrates a shift from restricting what students can access during online tests to supporting authentic demonstrations of capability within carefully controlled assessment environments. Five design tests are proposed for institutions: assessment validity, bounded tool access, humane participation, educator agency and reliable assessment delivery. The paper considers security and wellbeing together as design objectives. In the AI era, both are properties of assessment infrastructure that makes permitted assistance explicit and students' own capabilities meaningfully observable.



*Keywords:* academic integrity, digital assessment, digital wellbeing, generative AI, secure exams, authentic assessment


## Introduction

Generative artificial intelligence (GenAI) has highlighted a longstanding assessment challenge: a submitted piece of work does not always demonstrate the author's expertise. Australian sector guidance calls for assessment systems that both prepare students to work ethically with GenAI and provide meaningful points at which learning can be assured (Lodge et al., 2023, 2025). Because unauthorised GenAI use cannot currently be detected reliably, institutions can respond by clarifying permitted AI use, designing tasks that preserve valid evidence of learning, and directly supervising student performance (Lodge et al., 2025).

The need for secure assessment has therefore become a renewed institutional priority. Yet remote proctoring and surveillance-based systems have generated concerns about stress, inconsistent conditions, privacy and inequitable effects (Chung et al., 2024; Mutimukwe et al., 2026; Pokorny et al., 2023). These concerns do not remove the need to verify that assessment results reflect students' own learning; rather, they show that security cannot be judged solely by how extensively a system observes or restricts students.

This paper treats secure digital exams as educational infrastructure: technology, assessment design, governance and human support that together establish a trustworthy environment for demonstrating learning. It introduces digital exam wellbeing as a framework for asking: How can universities support valid, skills-based assessment without making surveillance or technical friction the organising logic of the examination? Several secure digital assessment tools are now moving beyond conventional browser lockdown to support controlled environments in which students can use approved applications, files and online resources. This paper examines that broader shift through an illustrative case, rather than evaluating the effectiveness of any particular platform.

This practice-informed conceptual paper draws on selected literature and descriptive material relating to the illustrative case. No participants were recruited, and no University pilot outcomes or identifiable student data are reported.

## From proctoring to configured assessment environments

Pandemic-era digital assessment included online examinations as well as open-book, take-home and oral formats. Lockdown browsers restricted navigation and local applications, while remote proctoring added identity checks and live monitoring. Highly restrictive configurations can be less suited to tasks involving discipline-specific tools and workflows (for example, analysing data, developing spreadsheets or models, writing and testing code, consulting approved sources, or producing files in professional software).

Authentic assessment asks students to apply knowledge, skills and dispositions to meaningful problems. Digital technologies can support authentic task design and capabilities for digitally mediated work (Hu et al., 2025), while authentic assessment has been associated with skill development, employability and academic integrity (Sotiriadou et al., 2020). Authenticity does not guarantee integrity, but applied tasks within known boundaries can provide evidence of how students use discipline-relevant tools and methods.

A configured assessment environment moves beyond simply restricting access by giving students the specific tools and resources needed to demonstrate the intended learning outcomes. Depending on the task, this may include an LMS assessment, selected websites, reference files, approved applications or a streamed virtual desktop, while tools and communication channels that would undermine the validity of the assessment remain restricted. The guiding question therefore shifts from “Is this exam locked down?” to “Does this environment allow what the task requires, restrict what would compromise the evidence, and remain usable?” This reflects constructive alignment: intended outcomes, learning activities and assessment should align (Biggs, 1996).

Assessment frameworks and institutional guidance increasingly differentiate among prohibited, restricted, disclosed and integrated uses of GenAI, depending on the intended learning outcomes and the role assigned to AI within the task (Ali et al., 2025; McDonald et al., 2025; Perkins et al., 2024). A configured workspace could support an AI-restricted assessment of unaided capability or an AI-inclusive assessment in which students’ responsible use of an approved service is evaluated.

## Illustrative case: the evolution of Safe Exam Workspace

The transition from browser lockdown to configured assessment environments is reflected in the evolution of contemporary secure assessment platforms. Schoolyear’s Safe Exam Workspace (SEW) provides one example of this broader development by supporting controlled access to approved applications, files and online resources (Figure 1). In its virtual desktop configuration, approved applications run remotely while the local endpoint is restricted.

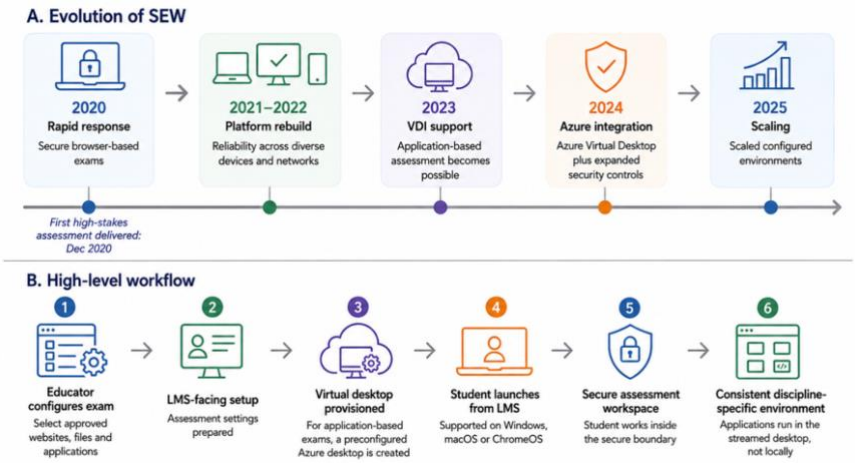



*Figure 1.* Evolution and workflow of Safe Exam Workspace (SEW). (A) SEW expanded from browser-based restriction to application-based assessment through virtual desktops. (B) Educators configure approved resources through an LMS-facing interface; a preconfigured desktop is provisioned through Microsoft Azure for student access

The case, based on descriptive information supplied by Schoolyear, highlights that secure assessment depends not only on restricting access, but also on reliable configuration, predictable delivery and manageable processes for educators, students and support teams. Schoolyear reported 140 customers across North America, Europe, Asia, Australia and New Zealand. Total examination sessions increased from 1,258,618 in July 2024–July 2025 to 2,355,382 in July 2025–July 2026; virtual desktop exams increased from 18,078 to 84,181, a 366% increase.

Schoolyear also reported adoption pathways ranging from faculty-led demand for application-based assessment to institution-wide procurement and the replacement of systems that were difficult to maintain or configure. These pathways illustrate that secure digital assessment is not solely a technical concern; its implementation must also account for pedagogy, institutional governance and operational support. The case therefore provides a practical basis for considering the broader institutional qualities captured in the digital exam wellbeing framework.

## Digital exam wellbeing as an infrastructure framework

Digital exam wellbeing concerns how secure assessment environments protect academic standards while minimising avoidable technical, cognitive, privacy or accessibility burdens on students. It also recognises that security measures are not neutral: preventable technical failures, unclear monitoring practices, inaccessible requirements and inconsistent examination conditions can affect student performance and weaken the validity of assessment results. The aim is not to eliminate the inherent pressure of high-stakes assessment, but to ensure that avoidable burdens do not interfere with students' ability to demonstrate their learning.

Evidence from remote-proctoring research illustrates these risks. In an analysis of 16,010 student responses, Chung et al. (2024) found that social and cultural factors shaped preparedness, stress and perceived performance, with proctoring amplifying some disparities. Pokorny et al. (2023) reported mental-health concerns and inconsistent remote examination conditions, while Mutimukwe et al. (2026) identified privacy concerns and emphasised the importance of involving students and educators in procurement and implementation. Although these studies focus on remote proctoring rather than secure digital assessment more broadly, they suggest that the burdens associated with security measures may fall disproportionately on some student groups.

We propose five sociotechnical design tests to guide institutional evaluation of digital exam wellbeing (Table 1). These tests cannot be satisfied by any product in isolation; they also depend on assessment design, institutional policy, network readiness, accessibility, staff capability, support and fallback arrangements.

*Table 1.*
Five design tests for secure digital exam infrastructure

| Design test | Institutional question | Examples of evidence to seek |
|---|---|---|
| Assessment validity and authenticity | Can students use the discipline-relevant tools needed to demonstrate the intended learning outcomes? | Alignment of tools and restrictions with outcomes; support for realistic files, applications and workflows; review by educators and students. |
| Bounded and intelligible tool access | Are permitted and prohibited resources explicit, consistently enacted and understandable? | Tested configurations; clear AI-use conditions; whitelisting behaviour; confirmation that a secure launch represents the approved environment. |
| Humane and equitable participation | Does the security model minimise avoidable cognitive, privacy, accessibility and device burdens? | Device checks and loan options; accessibility and language testing; proportionate data collection; student preparation; clear incident and appeal processes. |
| Educator agency with institutional guardrails | Can educators configure appropriate assessments without excessive dependence on specialist IT or unsafe local variation? | LMS-integrated setup; reusable configurations; preview and approval workflows; role-based access; centrally governed minimum security. |
| Operational reliability | Can the whole exam system recover predictably at scale? | Network and load testing; monitoring; restart and fallback workflows; trained supervisors; support coverage; retention, reporting and incident governance. |

The framework highlights two important relationships. First, usability contributes to security. When systems are difficult to configure or use, staff may weaken settings, students may avoid preparation processes, and faculties may turn to unsupported alternatives, ultimately reducing the reliability of secure assessment. Second, digital exam wellbeing depends on the broader institutional environment, not only on the student interface. Even a simple interface cannot prevent unnecessary burden if device requirements, privacy practices, accessibility arrangements, support processes and fallback procedures remain unclear or inadequate.

## Discussion and conclusion: infrastructure for skills-based and AI-inclusive assessment

Secure digital assessment should not be framed only as a contest between anti-cheating technologies and AI-enabled circumvention. That framing prioritises detection while leaving the nature of the assessed performance largely unchanged. The digital exam wellbeing framework instead directs attention to the capabilities students are expected to demonstrate, the resources required to demonstrate them, and the conditions under which the resulting evidence can be considered credible.

Configured workspaces can support students to analyse data, build models, edit code, interpret simulations or produce discipline-relevant files within defined conditions. Depending on the purpose of the assessment, students might work without AI to establish foundational capability or use an approved AI tool where evaluating, correcting or documenting its output forms part of the task. In either case, validity depends on whether the permitted resources and restrictions align with the intended learning outcomes.

Secure assessment infrastructure also creates responsibilities concerning privacy, device access, accessibility and operational support. Institutions should communicate data practices clearly, provide suitable alternatives where required, and ensure adequate technical support and fallback arrangements. Secure examinations are only one component of a broader assessment system, and their use should depend on the intended learning outcomes. Open-book, take-home, oral, project and portfolio assessments may provide more appropriate evidence in other contexts. Where controlled conditions are appropriate, secure examinations can provide

selected points at which students demonstrate capability under known conditions, alongside other inclusive and contextualised forms of evidence gathered across a program (Lodge et al., 2023, 2025).

The framework also broadens institutional decision-making. Procurement and implementation should consider not only technical controls, but also the assessment designs a system enables, the work required of educators and support teams, the governance of data and incidents, consistency across settings, accessibility and device requirements, and the capacity to enable approved AI access as readily as restricting or prohibiting AI use. Evaluation should therefore include assessment validity, student and staff experience, equity and evidence from live delivery.

Digital exam wellbeing is intended as a technology-neutral framework rather than an approach tied to any single platform. The five design tests should therefore be examined across different secure assessment technologies, institutional settings, disciplines and student cohorts. Further research is needed to determine which configurations best support valid skills-based assessment, equitable participation, educator agency, reliable delivery and responsible AI use, including approaches that reduce reliance on surveillance-intensive remote proctoring. Although wellbeing concerns in assessment predate GenAI, the AI era sharpens questions about permitted assistance and how students' own capabilities can be evidenced.

GenAI has intensified the need for trustworthy judgements about student learning, but it should not force a choice between unprotected assessment and surveillance-heavy restriction. Digital exam wellbeing instead asks what infrastructure allows students to demonstrate the intended capabilities, using appropriate tools, under clear and defensible conditions. By treating assessment validity, bounded access, humane participation, educator agency and operational trustworthiness as interdependent, the framework shifts attention from enforcement alone towards dependable, human-centred assessment infrastructure for an AI-mediated world.

## References

Ali, A., Collier, A. H., Dewan, U., McDonald, N., & Johri, A. (2025). Analysis of generative AI policies in computing course syllabi. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1* (pp. 18–24). Association for Computing Machinery. https://doi.org/10.1145/3641554.3701823

Biggs, J. (1996). Enhancing teaching through constructive alignment. *Higher Education, 32*(3), 347–364. https://doi.org/10.1007/BF00138871

Chung, J., Yu, A. S., & Henderson, M. (2024). Inequity in exam experience: Large-scale survey of proctoring and online exam experience by gender, internationality and language. In T. Cochrane, V. Narayan, E. Bone, C. Deneen, M. Saligari, K. Tregloan, & R. Vanderburg (Eds.), *Navigating the terrain: Emerging frontiers in learning spaces, pedagogies, and technologies. Proceedings ASCILITE 2024* (pp. 156–164). ASCILITE. https://doi.org/10.14742/apubs.2024.1229

Hu, A., Liu, Q., & Daniel, B. (2025). Digital technologies in authentic assessment in higher education: A systematic literature review and narrative synthesis. *SAGE Open, 15*(3), 1–27. https://doi.org/10.1177/21582440251357198

Lodge, J. M., Bearman, M., Dawson, P., Gniel, H., Harper, R., Liu, D., McLean, J., & Ucnik, L. (2025). *Enacting assessment reform in a time of artificial intelligence*. Tertiary Education Quality and Standards Agency. https://www.teqsa.gov.au/sites/default/files/2025-09/enacting-assessment-reform-in-a-time-of-artificial-intelligence.pdf

Lodge, J. M., Howard, S., Bearman, M., Dawson, P., & Associates. (2023). *Assessment reform for the age of artificial intelligence*. Tertiary Education Quality and Standards Agency. https://www.teqsa.gov.au/sites/default/files/2023-09/assessment-reform-age-artificial-intelligence-discussion-paper.pdf

McDonald, N., Johri, A., Ali, A., & Collier, A. H. (2025). Generative artificial intelligence in higher education: Evidence from an analysis of institutional policies and guidelines. *Computers in Human Behavior: Artificial Humans, 3*, Article 100121. https://doi.org/10.1016/j.chbah.2025.100121

Mutimukwe, C., Viberg, O., McGrath, C., & Cerratto-Pargman, T. (2026). Privacy in online proctoring systems in higher education: Stakeholders' perceptions, awareness and responsibility. *Journal of Computing in Higher Education, 38*, 732–761. https://doi.org/10.1007/s12528-025-09461-5

Perkins, M., Roe, J., & Furze, L. (2024). The AI Assessment Scale revisited: A framework for educational assessment [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2412.09029

Pokorny, A., Ballen, C. J., Drake, A. G., Driessen, E. P., Fagbodun, S., Gibbens, B., Henning, J. A., McCoy, S. J., Thompson, S. K., Willis, C. G., & Lane, A. K. (2023). "Out of my control": Science undergraduates report mental health concerns and inconsistent conditions when using remote proctoring software. *International Journal for Educational Integrity, 19*, Article 22. https://doi.org/10.1007/s40979-023-00141-4

Sotiriadou, P., Logan, D., Daly, A., & Guest, R. (2020). The role of authentic assessment to preserve academic integrity and promote skill development and employability. *Studies in Higher Education, 45*(11), 2132–2148. https://doi.org/10.1080/03075079.2019.1582015



Jativa, F. & Janic, F. (2026). From academic integrity to digital exam wellbeing: Reframing secure exam infrastructure in the AI era. In Cochrane, T., Narayan, V., Poole, T., Lai, P., Lake, P., Moore, O., & Li, L. (Eds.), *The Future is Connection: Collaboration, Creativity and Compassion in a Digital Society*. Proceedings ASCILITE 2026. Brisbane (pp. 648–653). https://doi.org/10.65106/apubs.2026.3414



Note: All published papers are refereed, having undergone a double-blind peer-review process.
The author(s) assign a Creative Commons by attribution license enabling others to distribute, remix, tweak, and build upon their work, even commercially, as long as credit is given to the author(s) for the original creation.

© Jativa, F. & Janic, F. 2026.