

NEGOTIATING USABILITY AND SECURITY IN DIGITAL TRANSFORMATION: A QUALITATIVE STUDY OF EVERYDAY WORK IN FINNISH VOCATIONAL EDUCATION

ANNA-LIISA OJALA,¹ TUOMO SIPOLA,² KARO SAHARINEN²

¹ Jamk University of Applied Sciences, School of Professional Teacher Education,
Jyväskylä, Finland
anna-liisa.ojala@jamk.fi

² Jamk University of Applied Sciences, Institute of Information Technology, Jyväskylä,
Finland
tuomo.sipola@jamk.fi, karo.saharinen@jamk.fi

This study examines how employees in Finnish vocational education institutions experience digitally mediated work and balance tensions between usability and digital security. Based on 25 qualitative interviews and complementary observations, the study shows that everyday work is shaped by fragmented digital environments, where multiple systems, changing interfaces, and external collaborations increase the complexity of work. The findings demonstrate that security measures, such as access restrictions and authentication practices, both enable and constrain work, often introducing friction into everyday tasks. In response, employees develop informal practices, including workarounds and the use of non-official systems, to maintain workflow. The findings show that employees continuously balance usability and security in fragmented multi-system environments shaped by changing digital systems and organisational boundaries. The study suggests that usability and security should be understood as continuously negotiated aspects of everyday digitally mediated work.

DOI

[https://doi.org/
10.18690/um.fov.4.2026.53](https://doi.org/10.18690/um.fov.4.2026.53)

ISBN

978-961-299-152-4

Keywords:

digital transformation,
usability–security tension,
vocational education,
shadow IT and
workarounds,
qualitative research



University of Maribor Press

1 Introduction

Digital transformation has reshaped everyday work across organisational settings, including educational institutions. In vocational education, work is increasingly mediated by a wide range of digital systems, services, and processes that structure how employees perform their tasks and interact with students, colleagues, and external stakeholders. Previous research has highlighted the importance of digital employee experience in understanding how workers interact with organisational technologies and digital environments (Moganadas & Goh, 2022). Studies on usability and security have shown a recurring tension between systems designed for efficient task completion and those enforcing strict security measures (Adams & Sasse, 1999; Norman, 2005a; Kaında et al., 2010; Agboola et al., 2024). While usability supports efficiency and user satisfaction, security measures such as authentication protocols and access restrictions may introduce friction into everyday work practices.

This tension is particularly relevant in vocational education institutions, where digital systems are used across pedagogical, administrative, and support functions and where work often involves collaboration with external actors such as guardians and public service providers. Vocational education also includes authentic work-based learning environments, such as training restaurants and workshops, where students interact with real customers and digital systems may involve handling customer data.

In addition, vocational education extends beyond educational institutions, as students complete practical training in workplaces and other organisations. This creates additional interfaces between organisational systems, practices, and data protection requirements. As vocational education is closely connected to working life, ongoing digitalisation across industries also shapes institutional digital infrastructures and employees' skill requirements (Busse et al., 2019).

Despite growing interest in digital transformation and employee experience, limited empirical research has examined how employees balance usability and digital security in everyday digitally mediated work. Previous research in vocational education has emphasised digital competences, including data protection and cybersecurity skills (Koramo et al., 2018; Paananen et al., 2023), while studies have also shown that digital transformation may be experienced as burdensome and contradictory

(Alanko-Turunen et al., 2024). This paper examines how employees in Finnish vocational education institutions experience digitally mediated work and balance usability and digital security in everyday practices. The study is based on qualitative interview data collected from three vocational education institutions and is guided by two research questions:

1. What kinds of digital systems and service environments shape everyday work in vocational education institutions?
2. How do employees negotiate tensions between usability and digital security in digitally transformed everyday work?

The study contributes to research on digital transformation by showing how fragmented system environments and security requirements shape everyday digitally mediated work in vocational education.

2 Theoretical background

Digital transformation has reshaped work environments through the increasing use of digital systems that mediate communication, information management, and task execution. These interactions form what has been described as the digital employee experience, referring to employees' engagement with organisational digital systems and processes throughout their work (Moganadas & Goh, 2022; Gheidar & ShamiZanjani, 2020). A key dimension of this experience is how usable employees perceive these systems to be.

Usability is commonly understood as the extent to which a system enables users to achieve their goals effectively, efficiently, and with satisfaction in a given context of use (ISO 9241-11:2018). In addition to effectiveness and efficiency, usability also includes dimensions such as learnability and memorability, which are particularly relevant in environments where employees must work with multiple systems and frequently changing interfaces (Kainda et al., 2010). These dimensions shape how smoothly employees can carry out their work and how easily they can adapt to new or evolving digital tools. In this study, usability is approached through the framework by Kainda et al. (2010), which conceptualizes usability through dimensions such as effectiveness, efficiency, satisfaction, learnability, and memorability. This framework

is particularly useful for examining how usability and security are intertwined in everyday work practices.

At the same time, digital work environments are increasingly shaped by requirements related to data protection, information security, and cybersecurity. Together, these requirements regulate how information is accessed, processed, shared, and protected in organisational digital environments (Maurer & Morgus, 2014; Althonayan & Andronache, 2018; Cains et al., 2022).

Previous research has consistently shown that usability and security are closely intertwined. Security mechanisms such as authentication procedures, access controls, and restrictions are designed to protect systems and data, but they may also complicate system use and introduce additional steps into work processes (Adams & Sasse, 1999; Norman, 2005b). Poor usability can lead users to bypass security measures, while overly strict security controls may hinder task performance and reduce system acceptance (Kainda et al., 2010; Lennartsson et al., 2021; Agboola et al., 2024). This creates a tension between usability and security, where improvements in one dimension may negatively affect the other.

Prior research has also identified the use of informal technologies and practices in organisational work. Shadow IT refers to systems or applications that are not officially approved by the organisation and often emerge when formal systems are perceived as restrictive or insufficient for everyday work (Silic & Back, 2014). Similarly, workarounds describe alternative ways of completing tasks when formal systems or procedures hinder work practices (Azad & King, 2008; Alter, 2014). While such practices may improve workflow efficiency, they may also introduce information security risks and reflect tensions between usability and security.

In complex organisational environments, such as vocational education institutions, this tension is further shaped by the diversity of roles, tasks, and system interfaces. Employees operate across pedagogical, administrative, and support functions, often in collaboration with external stakeholders. These conditions increase the likelihood that usability and security requirements come into conflict in practice. As a result, employees may use informal practices and non-official systems to maintain the flow of work when formal systems or security measures do not align with practical needs. This study examines how employees balance usability and security in everyday

digitally mediated work. Usability–security tensions emerge in situations where organisational requirements, work practices, and digital systems do not fully align.

3 Method

3.1 Data collection

The data consists of 25 thematic interviews (Amis, 2005), conducted in spring 2024 across three Finnish vocational education institutions operating in five locations. The total duration of the interviews was just under 22 hours, with individual interviews lasting on average slightly over 50 minutes. The interviews were conducted in Finnish and carried out by one or two members of the research team at a time. The interviews were mainly conducted individually; however, one was conducted as a small group interview with three participants. All participating institutions operated across multiple locations, and one of the institutions was a special needs vocational education provider.

The interviewees represented a range of organisational roles, including teaching staff, administrative personnel, IT and digitalisation specialists, student support services, and institutional leadership. This allowed the study to capture diverse perspectives on digitally mediated work across the organisation. The interview themes focused on employees' everyday work, the digital systems they use, and their experiences of usability and digital security. The interviews were semi-structured and followed a shared interview guide, while allowing flexibility for participants to describe their work practices and experiences in their own terms.

In addition to interviews, a small set of observations was conducted in selected learning environments within the participating institutions. The observations focused on everyday work practices and the use of digital systems in practice. These observations were used to support the interpretation of interview data, particularly in identifying situations where usability and security requirements come into tension.

All interviews were recorded and transcribed using the Whisper speech recognition system (Radford et al., 2023), implemented as a local solution so that the data did not leave the organisation's systems. The transcripts were subsequently reviewed and

edited manually. The data was anonymised during transcription to remove identifiable information related to individuals and organisations.

3.2 Data analysis

The data was analysed using qualitative thematic analysis (Braun & Clarke, 2006). The analysis proceeded in two phases. In the first phase, the interview transcripts were read and coded to identify recurring themes related to digital systems, work practices, and experiences of usability and security. The data was coded systematically following the research questions (Ruusuvuori et al., 2010). The coding process combined themes emerging from the interview data with concepts related to usability, security, workarounds, and shadow IT identified in previous research. Relevant excerpts were collected into an analysis document, where initial observations and interpretations were recorded. In addition, a table was constructed to map the digital systems mentioned in the interviews and the tasks associated with them. This supported the identification of patterns across roles and organisations.

In the second phase, the identified themes were further interpreted in relation to the concepts of usability and digital security. Particular attention was paid to situations where usability and security came into tension. The analysis focused on how employees described these situations and responded to them in everyday work. Through this process, the analysis identified patterns related to fragmented digital environments, security-related work constraints, and the use of informal practices and non-official systems to maintain workflow. These themes form the basis of the findings presented in the following section.

4 Findings

4.1 Fragmented digital work environment

The interview data shows that there is no single, shared digital work environment in vocational education institutions. Instead, employees work within a fragmented landscape of digital systems that varies across roles, tasks, and organisational contexts. This finding is in line with previous research highlighting the increasing complexity of digital environments in vocational education (e.g., Koramo et al., 2018; Paananen et al., 2023).

Interviewees described using a wide range of systems to carry out their work, including learning management systems, administrative platforms, communication tools, and specialised systems related to student support and external collaboration. The number and type of systems varied depending on the employee's role. Teaching staff emphasised learning platforms and communication tools, while administrative staff and IT specialists worked across multiple management and back-end systems. As a result, work is distributed across several digital systems, and even simple tasks may require the use of multiple platforms with different interfaces, logics, and requirements.

The data also shows that systems are not always well integrated. Employees described situations where the same information had to be entered into multiple systems or where systems did not communicate effectively with each other. This increases the complexity of work and creates uncertainty about where up-to-date information is located. These challenges require employees to develop practical ways of managing information across systems. The fragmented nature of the digital environment forms the context in which usability and security are experienced in practice. It also creates situations where employees must balance workflow efficiency, accuracy, and security-related organisational requirements.

4.2 Security measures as constraints on everyday work

Security-related requirements shape everyday work in vocational education institutions in multiple ways. The interview data shows that information security, data protection, and access control are embedded in digital systems and influence how employees can carry out their tasks. A central theme in the data concerns access rights and the management of information. Employees described situations where access to information is restricted in order to protect sensitive data, but where these restrictions may also complicate everyday work. Managing the balance between limiting access and enabling work was described as a continuous challenge. As one vice-rector noted, "The key issue is how to restrict information management and access rights in a way that does not prevent work tasks." This reflects the broader challenge of balancing usability and security in digital systems (Kainda et al., 2010; Agboola et al., 2024).

In practice, security measures such as access restrictions, authentication procedures, and system-specific permissions introduce additional steps into work processes. These measures are intended to ensure compliance and protect data, but they can also slow down work or make it more cumbersome. Employees described situations where they needed to log into multiple systems, manage different credentials, or navigate restrictions that limited their ability to access or share information when needed.

More concretely, the data provides several examples of how these security measures may constrain work in practice. Technical requirements such as VPN connections may, in some cases, prevent work altogether when systems fail. As one administrative staff member described: “The VPN didn’t work during those in-between days... fortunately, I had taken paper documents, which I then archived. The system just didn’t work... I simply couldn’t do my job.”

Similarly, multi-factor authentication (MFA), while recognised as an important security mechanism, was often experienced as frustrating and disruptive to workflow. A vocational teacher described the use of multi-factor authentication the following way: “Two-factor authentication has now been introduced. It’s frustrating! The phone isn’t necessarily right next to you, so you have to go and get it.”

Access control mechanisms also emerged as a source of tension. While restricting access to information is essential for data protection, employees reported that access rights do not always align with practical work needs. In some cases, restricted access made it more difficult to obtain necessary information, while in others, broad access created challenges in managing large amounts of visible data. Many interviewees, particularly those working in administrative roles, reported that in some situations they had access to more information than necessary:

Interviewer: That was perhaps the next question — do you feel that you sometimes see too much information?

Interviewee: Yes, definitely. Yes, I do... although, of course, it’s not really... well.

Interviewer: I suppose you also become somewhat desensitized to that information?

Interviewee: Yes. I mean, yes - it becomes normal that everything just sort of appears all at once.

At the same time, many of these professionals noted that it is part of employees' professional competence to manage this exposure to information without becoming overwhelmed.

The data also highlights situations where secure system use conflicts with the practical demands of work. Interview data and observations both point to such situations. For example, in some learning environments, such as simulated workplaces within educational settings (including settings like on-campus training restaurants or automotive workshops) digital systems may contain sensitive customer data. At the same time, the smooth running of work may require systems to remain easily accessible to multiple users. In such situations, practices that support workflow efficiency often conflict with data protection requirements and introduce security risks.

These findings indicate that security is not experienced as a separate layer of digital systems, but as something that directly shapes how work is carried out. Security measures can both enable and constrain work, and employees must continuously navigate these constraints in order to complete their tasks.

4.3 Informal practices and shadow IT

The data shows that employees do not rely solely on officially provided systems and practices in their work. Instead, they develop informal ways of working and use non-official tools to support task completion when formal systems do not adequately meet their needs. One form of this is the use of tools that are not part of the organisation's official system environment. As one vice principal described, their institutional work relies on a set of core systems, such as Microsoft 365 and the organisation's Moodle environment, which are largely under institutional control. At the same time, employees make extensive use of a wide range of third-party applications in teaching, communication, and everyday work. These systems fall outside institutional oversight, making it difficult to monitor their use or manage data within them. As the interviewee emphasised, this requires employees to develop an understanding of what kinds of information can be shared across different

platforms. Notably, the interviewee did not advocate for strict prohibition, but rather for informed and responsible use of systems. In this case, the institution also provided support for the use of non-core systems, viewing this as a more secure approach than attempting to prohibit their use altogether.

In addition, employees described using various communication tools to coordinate work, communicate quickly, or share information in situations where official systems were perceived as too slow, complex, or restrictive. The messaging application WhatsApp was widely mentioned in the data as an example of shadow IT. Although its use for work-related purposes was explicitly prohibited in two of the participating institutions, employees nevertheless used it in practice when necessary. As one teacher noted: “We are not allowed to use WhatsApp... however, teachers still use it via their personal phones to communicate with students, as it remains the most effective communication channel.”

In addition to using non-official systems, some employees described adapting their use of digital systems and practices to better fit the demands of everyday work. Employees developed these adaptations when formal systems did not fully support everyday work tasks. These findings indicate that these informal practices are closely linked to the tension between usability and security. When formal systems are perceived as difficult to use or when security measures restrict access or slow down work, employees seek alternative ways to complete their tasks. In this sense, shadow IT and workarounds emerge when system design does not align with everyday work requirements. At the same time, these practices may introduce new risks. The use of non-official systems can challenge organisational control over data and communication, while workarounds may bypass intended security mechanisms. Employees balance workflow efficiency against data protection and information security requirements in these situations. This interpretation aligns with previous research on shadow IT and workarounds in organisational settings (Silic & Back, 2014; Alter, 2014).

4.4 External interfaces and system change

The data indicates that digitally mediated work in vocational education institutions is not limited to internal systems, but it extends to interactions with external actors and systems. Employees operate in environments where information must be shared

across organisational boundaries, including collaboration with students' guardians, workplaces where students complete their practical training, and public sector organisations such as healthcare providers when students require additional support. These external interfaces introduce additional complexity to digital work. The different organisations use different systems, follow different practices, and apply different requirements related to data protection and information sharing. As a result, employees must navigate not only in their own organisation's digital environment, but also those of external partners.

The findings also highlight the impact of ongoing system changes. Employees described situations where new systems are introduced, existing systems are updated, or processes are modified. These changes require continuous adaptation and learning, and they may temporarily disrupt established work practices. More concretely, interviewees described how multiple systems and digital processes had changed within a relatively short period of time, requiring them to continuously learn new functionalities alongside their regular work tasks. In some cases, this led to situations where not all information was recorded in systems, as employees did not have sufficient time to fully adopt new practices.

In addition, system updates and interface changes were reported to occur without prior notice, forcing employees to adapt abruptly to new layouts and functionalities. For example, interviewees described situations where familiar interface elements, such as buttons or menu structures in systems like learning management platforms or administrative tools, changed unexpectedly. This reduced memorability and increased cognitive load by previously learned routines.

Together, external interfaces and system changes increase the complexity of digital work and intensify the tension between usability and security. Employees must continuously adjust their practices in response to changing systems, evolving requirements, and the need to coordinate work across organisational boundaries. Technologies, organisational structures, and everyday work practices continuously shape how usability and security are realised in practice.

5 Discussion & Conclusion

The findings contribute to existing research on the relationship between usability and security by showing how this tension is experienced and managed in everyday work practices. Previous studies have demonstrated that security mechanisms may reduce usability and lead users to bypass or resist system constraints (Adams & Sasse, 1999; Kainda et al., 2010; Norman, 2005; Agboola et al., 2024). This study shows that usability and security emerge through everyday work practices, organisational requirements, and interactions with digital systems. Employees continuously balance workflow efficiency, access to information, and security requirements in their daily work.

In the studied setting, employees continuously balance the need to protect information with the need to perform their tasks efficiently. Security requirements are not experienced as separate from work but as embedded in everyday practices. The usability–security tension is situational and shaped by specific work tasks, organisational contexts, and system environments.

The findings also contribute to research on shadow IT and workarounds by showing how these practices emerge in response to mismatches between formal systems and everyday work requirements. Prior research has conceptualized shadow IT as the use of non-approved systems (Silic & Back, 2014) and workarounds as informal practices that enable task completion despite system constraints (Alter, 2014; Azad & King, 2008). The results of this study support these perspectives.

In this study, informal practices emerge when formal systems do not adequately support everyday work. Employees adapt their use of systems and introduce alternative tools to maintain workflow continuity.

The findings further show that digitally mediated work in vocational education is shaped by interactions across organisational boundaries and by continuous system changes. Employees must coordinate work with external actors, including guardians, training workplaces, and public sector organisations, which introduces additional complexity to digital work environments. This supports previous research of Gheidar & ShamiZanjani (2020) and Moganadas & Goh (2022), which emphasises

that digital employee experience is shaped by digital interactions between employees, technologies, and the organisational environment.

The findings also have practical implications for organisations managing digitally mediated work. Digital systems and security measures should support everyday work practices across organisational boundaries and multi-system environments. Particular attention should be paid to reducing fragmentation between systems, aligning access controls with practical work needs, and supporting secure use of third-party applications instead of relying solely on prohibitions. However, the study is limited to Finnish vocational education institutions and qualitative interview data, which provide contextual depth but do not support broad generalisation. Future research could examine similar usability–security tensions in other organisational settings and through longitudinal or comparative approaches.

This study contributes to research on digital work by showing how employees balance usability and security in complex multi-system environments. The findings demonstrate how fragmented digital infrastructures, organisational boundaries, and continuous system changes shape everyday digitally mediated work in vocational education. The findings underline the importance of designing and managing digital systems in ways that align with the realities of everyday work. In vocational education, this complexity is further intensified by the integration of work-based learning environments and cross-organisational collaboration.

References

- Amis, J. (2005) Interviewing for case study research. In D. L. Andrews, D. S. Mason & M. L. Silk (Eds.) *Qualitative methods in sports studies*, Berg, pp. 104–138.
- Adams, A. & Sasse, M. A. (1999) Users are not the enemy. *Communications of the ACM*, 42 (12), 40–46. <https://doi.org/10.1145/322796.322806>
- Agboola, T. O., Adegede, J. & Jacob, J. G. (2024) Balancing usability and security in secure system design: A comprehensive study on principles, implementation, and impact on usability. *International Journal of Computing Sciences Research*, 8, 2995–3009.
- Alanko-Turunen, M., Heinilä, H. & Vainio, V. (2024) Developing digitalizing practices in vocational education – Integrating digitalization and emotions [in Finnish]. *eSignals Research*, 5 (1). <http://urn.fi/URN:NBN:fi-fe202402055586>
- Althonayan, A., & Andronache, A. (2018) Shifting from information security towards a cybersecurity paradigm. *Proceedings of the 2018 10th International Conference on Information Management and Engineering*, 68–79.
- Busse, J., Lange, A. & Schumann, M. (2019) Effects of Digitalization on Vocational Education and Training: First Results of a Qualitative Study. In N. Pinkwart & J. Konert (Eds.) *DELFI 2019*, 67–72. Bonn: Gesellschaft für Informatik. https://doi.org/10.18420/delfi2019_206

- Cains, M. G., Flora, L., Taber, D., King, Z. & Henshel, D. S. (2022) Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42 (8), 1643–1669.
- Gheidari, Y. & ShamiZanjani, M. (2020) Conceptualizing the digital employee experience. *Strategic HR Review*, 19 (3), 131–135.
- Kainda, R., Flechais, I. & Roscoe, A. W. (2010) Security and usability: Analysis and evaluation. *Proceedings of the 2010 International Conference on Availability, Reliability and Security*, 275–282.
- Koramo, M., Brauer, S., & Jauhola, L. (2018) Digitalization in vocational education [in Finnish]. Finnish National Agency for Education, Reports and surveys 9.
- Lennartsson, M., Kävrestad, J. & Nohlberg, M. (2021) Exploring the meaning of usable security – A literature review. *Information & Computer Security*, 29 (4), 647–663.
<https://doi.org/10.1108/ICS-10-2020-0167>
- Maurer, T. & Morgus, R. (2014) Compilation of existing cybersecurity and information security related definitions. Washington: New America.
- Moganadas, S. R. & Goh, G. G. G. (2022) Digital employee experience constructs and measurement framework: A review and synthesis. *International Journal of Technology*, 13(5), 999–1012.
<https://doi.org/10.14716/ijtech.v13i5.5830>
- Norman, D. A. (2005a) Human-centered design considered harmful. *Interactions*, 12 (4), 14–19.
<https://doi.org/10.1145/1070960.1070976>
- Norman, D. A. (2005b) *The Design of Everyday Things*. Revised edition. New York: Basic Books.
- Paananen, H., Taivassalo, M., Raitanen, T., & Nieminen, A.-P. (2023). *Digital competence in vocational education – A guide for articulating competence* [in Finnish]. Finnish National Agency for Education.

About the authors

Anna-Liisa Ojala, PhD, Adjunct Professor (Title of Docent in Finland), works as a Senior Advisor at the Professional Teacher Education College at Jamk University of Applied Sciences, Finland. Her work focuses on researching and developing teachers' everyday work and examining the digitalisation of work and learning.

Tuomo Sipola, PhD, is a Principal Researcher at the Institute of Information Technology at Jamk University of Applied Sciences, Finland. His expertise includes artificial intelligence, machine learning, and cybersecurity, particularly the use of AI in cyber defence and digital security research.

Karo Saharinen, PhD, is a Senior Lecturer at the Institute of Information Technology at Jamk University of Applied Sciences, Finland. He is responsible for pedagogical development at the institute and works in the fields of cybersecurity, computer networks, and digital security education.

Summary

This study examined how employees in vocational education institutions experience and manage usability and security in digitally mediated work. The findings show that digital work is characterized by fragmented system environments in which employees operate across multiple platforms with varying functionalities and requirements. Security measures, such as access restrictions and authentication procedures, play a central role in shaping everyday work and may at times constrain task completion. In response, employees develop informal practices and rely on non-official systems to maintain workflow, particularly when formal systems do not adequately support their tasks. The findings also highlight that digital work extends beyond organizational boundaries and is continuously shaped by system changes and external collaboration. More broadly, the study suggests that vocational education institutions do not have a unified digital work environment. Instead, everyday digital work varies across roles, tasks, and organizational contexts, resulting in diverse and role-dependent employee experiences.