

Information privacy awareness and personal information management practices: A study of Indonesian students in Türkiye

Mindy Syailah Nurthoyyibah^{1*} and Özgür Külcü¹

¹ Information Management, Faculty of Letters, Hacettepe University, TÜRKİYE

Email: *mindynurthoyyibah@hacettepe.edu.tr (corresponding author);

kulcu@hacettepe.edu.tr

ORCID ID: Mindy Syailah Nurthoyyibah: <https://orcid.org/0009-0000-5283-5059>

Özgür Külcü: <https://orcid.org/0000-0002-2204-3170>

ABSTRACT

This study investigates Information Privacy Awareness (IPA) and Personal Information Management (PIM), focusing on Indonesian students in Türkiye, using an explanatory sequential, mixed-methods design. Survey was collected using a validated scale and analyzed using descriptive statistics and Spearman correlation test among 136 students. Interview data were used to contextualize the survey findings, including a comparison between individuals with higher and lower levels of IPA. Students reported a high overall level of privacy awareness, although the dimensions were unevenly developed. By integrating survey and interview evidence, the study showed that privacy awareness is associated with, but does not determine, consistent personal information management practice in the transnational academic context. Students were more proficient in basic protective behaviors than in technically demanding practices such as encryption and cookie management. Higher awareness group was associated with broader protective strategies, whereas lower awareness group was marked by reactive, convenience-oriented practices. Educational interventions may therefore need to move beyond awareness-raising initiatives toward the cultivation of applied competencies in secure file management, encryption, access control, and systematic personal information organization.

Keywords: Data privacy; Personal digital archive; Personal information security; Privacy protection; Students information behavior.

INTRODUCTION

Digital technology has changed the way people create, access and manage information. For example, when using university learning systems, social media or other applications and services, data is often collected. These changes present many opportunities but also serious risks, especially in relation to privacy, security and the misuse of personal data. Cybersecurity threats, one of the world's greatest challenges, have been reported worldwide. (Heading & Cavaciuti-Wishart, 2024). Therefore, it is important for people to be aware of information privacy and to learn how to manage their personal data appropriately. College students are exposed to new technology. They are frequent users of digital platforms, and they are

expected to be digitally literate. Research, however, shows that students do not always apply their knowledge about personal data rights and protection in practice (Eroğlu, 2018). Some studies suggest that students are aware of the importance of protecting their personal data but do not always translate this knowledge into action. This raises the question of how knowledge can be translated into practice; the gap between knowing and doing is central here.

Two interrelated concepts are critical to understanding this issue: Information Privacy Awareness (IPA) and Personal Information Management (PIM). IPA is defined as an individual's awareness of privacy risks, control over personal data, and responsible information-sharing behaviour. PIM, on the other hand, refers to the activities that individuals engage in to organise, store, retrieve, secure, and manage their personal information. These concepts are connected, but no detailed study has yet examined their relationship. As stated by Külcü and Henkoğlu (2014, p. 232), proper digital information management is a method for safeguarding personal data that relies on the informed behaviour of data owners. Yet it is unclear whether higher levels of privacy awareness always lead to more effective information management practices.

The phenomenon is more complex for international students. Existing studies highlight that migrants and international students encounter additional challenges in managing personal information, including issues with accessing, organising, and protecting their data (Krtalić & Ihejirika, 2022; Chaudhry & Alajmi, 2024). Previous studies have addressed digital privacy and PIM separately, but few have examined the relationship between IPA and PIM among Indonesian students in Türkiye. Therefore, the present study attempts to address this gap by investigating the relationship between IPA and PIM practices among Indonesian postgraduate students in Türkiye. Specifically, it investigates how privacy awareness is reflected in students' information management behaviours and whether these patterns differ according to length of residence. The study employs an explanatory sequential mixed methods design to determine statistical relationships among variables and to offer a holistic understanding of the underlying behavioural patterns. In line with the purpose of the study, the research questions were formulated as:

- i. What are the levels of information privacy awareness (IPA) among Indonesian postgraduate students in Türkiye?
- ii. What are the levels and patterns of personal information management (PIM) practices among Indonesian postgraduate students in Türkiye?
- iii. Is there a statistically significant relationship between IPA and PIM practices among Indonesian postgraduate students in Türkiye?

LITERATURE REVIEW

International students' information behaviours

Information behaviour is an individual's habitual pattern of searching for, browsing, organising, sharing, and using information. International students exhibit unique information behaviours, and these behaviours change as they adapt. Information needs and the contexts in which they arise are constantly evolving. However, even when information demands are urgent, access to information is shaped by linguistic, cultural, social, digital, and other support-system barriers to meeting those needs (Youm et al., 2026). Gao's (2023) study on the information-seeking behaviour of international students in China demonstrated that their behaviour is shaped by a variety of experiences, habits, cultures, languages, academic backgrounds, and life experiences in the face of uncertainty, rather than by a single

pattern. This is likely to affect their privacy-related search behaviour and its relationship to the management of students' personal information. Thus, with the increasing importance of privacy literacy in addressing cybersecurity threats, greater attention is warranted internationally to address gaps in non-credible and outdated information, as well as in information search and management skills, that will further exacerbate associated risks (Youm et al., 2026).

Information privacy awareness

Historically, privacy research has sought to clarify privacy within domains such as social relations, technology, culture, politics, and law. Stone et al. (1983) defined privacy as 'the individual's ability to personally control information about oneself'. This definition suggests that individuals can mitigate potential risks by increasing control over their information, managing sensitive information, and anonymising it. The accessibility of data and information owned by individuals increases the risk of disclosure by third parties; therefore, protective measures should be taken to prevent the disclosure of personal information that should remain confidential (Joinson et al., 2010). Privacy has also been conceptualised as the right to express opinions without surveillance, the authority to determine whether to share or store personal information, the right to refuse recording or photography, the right to avoid digital or physical disturbance, the right to protect one's reputation, and the right to be shielded from unwarranted searches. Accordingly, privacy extends beyond individual concerns to include the regulation of others' access to information. Information privacy, the central focus of this study, is directly related to the processes of collecting, storing, processing, organising, and sharing personal data (Fatima et al., 2019).

Personal information, sensitive content, browsing history, messaging, conversations, and screenshots are now automatically uploaded to centralised social servers. According to Choi et al. (2017), there are significant security risks and threats in the digital ecosystem because such data is directly tied to personal privacy. Both internal and external threats are made possible by the ease with which sensitive data can be accessed and misused. Third parties' intentional acts against user information are the main source of external risks. Fraud, phishing, information theft, data sabotage, spying, manipulation, ad targeting, data selling, spam messaging, and device entry through cyberattacks are examples of these risks. Individuals are sometimes coerced through psychological manipulation into disclosing sensitive information about their relatives or close groups. However, most internal risks are caused by personal errors. According to Zhang et al. (2014) and Kani-Zabihi and Helmhout (2012), actions such as a lack of awareness of information security, accepting privacy rules without carefully reading them, insufficient knowledge of legal regulations, or careless data exchange lead to privacy infractions.

Compared to other age groups, university students at higher education institutions are expected to be more literate and more aware of digital privacy. Research by Korkmaz et al. (2021) assessed university students' awareness of internet privacy along three fundamental characteristics. First, the attention dimension refers to the extent to which students review and adjust their privacy settings to avoid disclosing excessive personal information. The security dimension then examines the behavioural and technical precautions students take to prevent the misuse of data and information in online settings. Finally, the communication and sharing dimension captures students' attitudes and behaviours regarding how they disclose and distribute their digital data and information. Students with high awareness are more cautious when disclosing information, aware of privacy restrictions, and accountable for the sensitive content they consume and distribute.

Personal information management

Information management can be evaluated from three main perspectives: organisational information management, library information management and personal information management (Detlor, 2010, p. 103). According to Detlor, personal information management enables individuals to increase their productivity by organising information related to education, careers, organisational operations and daily life. Building on this, Jones and Teevan (2007, p. 462) define personal information as information that is owned by, related to, under the control of, communicated by, stored by and offered to the individual. Personal information can shape cultural identity among migrants (Krtalić & Alon, 2024), especially those undergoing cultural transition, such as students studying abroad. Despite this, increasing technological complexity makes it difficult for individuals to manage their information effectively. As van Knippenberg et al. (2015) state, individuals who lack effective information management skills face obstacles such as information overload, difficulties in decision-making, and distraction when accessing the right information.

Personal digital content management is considered a part of PIM. Koçak (2021) defines the concept as a process that includes activities related to the organisation, storage, search and access, and deletion of information owned by individuals. This definition primarily overlaps with the statements of Barreau (1995) and Jones and Teevan (2007), who proposed PIM models. However, based on Koçak's research, the concept of 'digital content' is particularly emphasised. Koçak uses the term 'digital content' to refer to the management of content such as organising, erasing, searching and retrieving, ensuring privacy, backing up, and managing course documents. This concept spans various digital formats, including documents, photos, videos and other digital information, and incorporates aspects of digital literacy. Other models are not limited to digital content but also include physically accessed documents and personal information. Furthermore, the scale developed enables the measurement of students' PIM skill levels (in terms of operations such as editing, erasing, preserving and storing) and includes privacy and digital literacy elements. The scale is structured on the concepts of personal digital libraries, personal digital collections, personal digital archiving and PIM, as introduced by Karanikolas and Skourlas (2014, as cited in Koçak, 2021, p. 71).

METHODS

Research Design

This study employed an explanatory sequential mixed-methods design, in which quantitative data collection and analysis were followed by a qualitative phase aimed at explaining and deepening the quantitative findings (Creswell, 2009, p. 188). The purpose of the quantitative phase was to identify broad trends in both PIM and IPA, and to investigate further the relationship between IPA and PIM. The qualitative phase specifically examined how students with high and low level of privacy awareness understand and explain their daily PIM behaviours, thereby supporting a deeper analysis.

Sampling

The quantitative phase involved 136 Indonesian postgraduate students enrolled at universities in Türkiye. Participants were selected through criterion-based purposive sampling according to the following criteria: i) Indonesian students studying in Türkiye, and ii) enrolment in a postgraduate programme. Data collection was conducted via online distribution channels, such as student networks and online discussion groups.

From the survey, 20 participants were selected for interviews based on their total scale scores. A 5-point Likert scale was applied to a total of 55 items across both scales. The combined total score ranged from 54 to 275, after the negatively worded items had been appropriately reverse-coded. Cumulative scores integrating IPA and PIM practices were calculated to select participants for the interview sessions. The participants were then divided into two groups, as shown in Table 1. This purposive sampling was used in this study to more accurately capture participants' IPA and PIM experience levels. Using SPSS, quartiles were calculated based on the distribution of the survey responses (N = 136). To reach data saturation, an interview sample size of 5–25 participants is recommended (Creswell, 1988, as cited in Sharma et al., 2024, pp. 134–135).

Table 1: Criteria for the interview selection

Group	Total items	Selection criteria
High Awareness C (HAG) N=10	55 items total (IPA and PIM scales)	Top quartile (75th percentile and above, ≥ 235)
Low Awareness Group (LAG) N=10	5-point Likert scale - Range: 54-275	Bottom quartile (25th percentile and below, ≤ 192)

In addition to providing a qualitative explanation for the differences observed in earlier quantitative data, this quartile-based classification enabled a systematic comparison of contrasting awareness levels. The highest-scoring member of the HAG and the lowest-scoring member of the LAG were contacted first, followed by others who met the score criteria. This procedure was repeated until each group's quota of ten participants was reached.

Research instrument

A survey questionnaire comprising two validated scales is shown in Appendix 1. The IPA is measured by three dimensions: attention, security, and communication. The PIM is assessed via seven activities: organisation, deletion, search and access, privacy, backup, course document management, and digital literacy. Both scales were adapted from established, previously validated instruments, with the IPA scale drawn from Korkmaz et al. (2021) and the PIM scale from Koçak (2021). Cronbach's alpha values greater than 0.794 (Korkmaz et al., 2021) indicate acceptable internal consistency in accordance with recognised reliability standards. The overall PIM scale's alpha value of 0.70 (Koçak, 2021) also exceeds this threshold. Semi-structured interviews were conducted to gather qualitative data.

Data collection procedures

The survey questionnaire, comprising the IPA and PIM scales together with demographic questions, was administered through Google Forms and distributed to Indonesian postgraduate students in Türkiye between March and April 2025. After a preliminary analysis of the survey data, the respondents were grouped to HAG and LAG based on their total scores. The interviews were conducted with the respondents in these groups with Each interview lasted approximately 20 to 40 minutes.

Data analysis

SPSS software was used to clean, process and analyse the quantitative data. To ensure consistency in scoring, negative items on both scales were suitably reverse coded prior to

analysis. Participants' overall IPA and PIM levels were assessed using arithmetic mean scores on a five-point Likert scale (where 1–2 represented negative responses, 3 represented neutral responses, and 4–5 represented positive responses). To systematically determine low, moderate and high levels based on mean scores of students' IPA and PIM, the following classification criteria and cut-off points were applied.

Table 2. Classification criteria and cut-off points for IPA and PIM mean scores

Mean score	Classification	Interpretation
1.00–2.33	Low	Low level of privacy awareness or inconsistent personal information management behaviour
2.34–3.67	Moderate	Moderate level of privacy awareness and moderately consistent personal information management behaviour
3.68–5.00	High	High level of privacy awareness and consistent personal information management behaviour

Descriptive statistics, such as means and standard deviations, and inferential statistics were used to answer the research questions. The significant association between IPA and PIM practices was examined using Spearman's rank correlation analysis. NVivo 12 was used to conduct a thematic analysis of the qualitative interview data, following the framework developed by Braun and Clarke (2012). Qualitative data were used to contextualise, explain, and enhance the quantitative results in accordance with the explanatory sequential design. The qualitative data provided insight into the behavioural patterns underlying the observed statistical links and facilitated the identification of gaps between awareness and practice.

RESULTS

i. Information Privacy Awareness (IPA)

Responses across the three dimensions of Information Privacy Awareness (IPA) - attention, security, and communication indicate an overall pattern of moderate-to-high awareness, as shown in Table 3. The strongest agreement was observed in relation to the use of strong passwords, awareness of privacy threats, and the possibility of shared information being misused. According to the survey results, students' overall IPA was high ($M = 3.90$, $SD = 0.639$). The strongest dimension was Attention ($M = 4.28$, $SD = 0.775$), while Security ($M = 3.59$, $SD = .860$) and Communication ($M = 3.64$, $SD = .858$) were moderate. Thus, the overall high score should be interpreted as a combination of strong awareness of privacy-related risks and comparatively less consistent application of technical and communication-related controls.

The survey results reveal clear differences among IPA dimensions. Attention received the highest mean score ($M = 4.28$, $SD = 0.775$), indicating that students generally pay attention to privacy settings, notifications, passwords, and potential privacy risks. The survey results also indicate that students were most aware of the possibility that information shared online may be exploited by malicious individuals ($M = 4.39$, $SD = 0.920$). This finding implies that privacy protection awareness is influenced by several factors. Interview responses validate this, suggesting that students' understanding of privacy may stem from knowledge sharing,

reading, cultural background, and personal or others' experiences. As articulated by one interviewee:

"Since we are hearing more and more about fraud instances, I have recently come to understand how crucial it is to protect personal information" (LAG01)

Table 3. Level of information privacy awareness

Information privacy awareness (IPA)				
Dimension	Item	Mean	SD	Level of IPA
Attention	I check the privacy settings and notifications of the online platforms I use.	4.22	.946	High
	I set the privacy settings for my accounts on the online platforms I use (social networks, shopping sites, games, etc.).	4.36	0.948	High
	I make sure the passwords I use online are strong (using upper-case and lower-case letters, numbers, special characters, and at least eight characters).	4.35	0.905	High
	I can tell whether the content of messages I receive by email or on social media is reliable.	4.34	0.871	High
	I understand whether messages or emails from people I do not know in online environments pose a security risk.	4.14	1.019	High
	Information I share online may be accessed by companies, government agencies, or hackers.	4.22	0.978	High
	I am aware that the information I share on online platforms may be used by malicious individuals.	4.39	0.920	High
	Attention	4.28	0.775	High
Security	I am aware of the cookies used by websites.	3.26	1.115	Moderate
	When installing an app on my mobile device, I pay attention to the permissions it requests.	3.90	1.108	High
	I check the security certificates and data encryption methods of websites and mobile applications.	3.25	1.184	Moderate
	I check the security of the websites I visit.	3.86	0.944	High
	I pay attention to what information browser extensions will access.	3.73	1.014	High
	Security	3.59	0.860	Moderate
Communication	I share my personal information (address, date of birth, age, occupation, phone number, etc.) with people I do not know in online environments.	3.66	1.247	Moderate
	I share screenshots of my conversations with friends or relatives without asking for permission.	3.13	1.168	Moderate
	I share information, pictures, videos, and other content belonging to others online without asking for permission	3.39	1.225	Moderate
	I allow people I do not know to follow me or add me as a friend online.	4.30	1.092	High
	I communicate with people I do not know in online environments.	3.69	1.200	High
	Communication	3.64	0.858	Moderate
Overall IPA mean		3.90	0.639	High

*Note: 1 = Strongly disagree; 2 = Disagree; 3 = Neutral; 4 = Agree; 5 = Strongly agree

In contrast, security recorded a moderate score ($M = 3.59$, $SD = 0.860$). Within the security dimension, the lowest mean score was recorded for the statement “I check the security certificates and data encryption methods of websites and mobile applications” ($M = 3.25$, $SD = 1.184$). This result indicates a contrast between the attention and security dimensions, suggesting that students' alertness to privacy risks is not matched by equally developed protective actions. The interview findings help explain this difference. For example, HAG05 reported using management options to limit or reject cookies, whereas LAG05 stated that they had never heard of encryption methods or security certificates. This evidence suggests that students are more familiar with basic protective actions than with technically demanding privacy mechanisms. The pattern is therefore not simply a lack of privacy awareness; rather, it indicates that awareness is translated unevenly into technical practice.

“I accepted them all because I don't really care about cookies. I also had never heard of encryption methods, security certificates, or their dangers” (LAG05)

“I use research-specific management options to limit or reject cookies” (HAG05)

The communication dimension also recorded a moderate score ($M = 3.64$, $SD = 0.858$). The findings reveal inconsistency in how students safeguard personal data in their communication with others. This is illustrated by the statement “I share information, pictures, videos, and other content belonging to others online without needing to ask for permission” ($M = 3.39$, $SD = 1.2247$), which implies that protecting the privacy of others' data is often given low priority. These findings indicate that this pattern is influenced by competing social and personal considerations. HAG01 reported sharing information and documents only with certain people, demonstrating selective control over information disclosure. In contrast, LAG06 explained that privacy settings were not always used because social media was considered important for personal branding, while LAG08 reported using social media for work-related purposes while avoiding private information. Together, these findings indicate that students do not treat privacy as an absolute restriction on communication; rather, privacy decisions are negotiated against academic, professional, and self-presentation needs, which is particularly relevant for students studying abroad and maintaining academic and social networks across contexts.

“I share information and documents with certain people” (HAG01)

“I don't use privacy settings in my social media or other platforms because I need space for my personal branding” (LAG06)

“I use social media for work-related reasons, but I take care not to post private information” (LAG08)

Overall, the survey and interview findings indicate that students possess substantial conceptual awareness of information privacy, but the translation of this awareness into practice varies by context and type of activity. The difference between the high attention score and the moderate security and communication scores is important: students may recognise privacy risks without consistently applying technically demanding controls or restricting disclosure when social and professional benefits are perceived. For Indonesian postgraduate students studying in Türkiye, these decisions may occur across academic platforms, social media, and transnational communication networks, making privacy management a practical negotiation between protection, accessibility, and visibility rather than a single, uniform behaviour.

ii. Awareness level of Personal Information Management (PIM)

The survey results indicate a high overall level of PIM practices ($M = 3.79$, $SD = 0.702$). However, the dimension-level results reveal uneven development of PIM across key activities that underpin management effectiveness. For instance, Organisation recorded a high mean ($M = 4.28$, $SD = 0.775$), whereas Privacy ($M = 3.64$, $SD = 0.858$) and Information Search and Access ($M = 3.59$, $SD = 1.060$) were Moderate. Thus, The overall PIM Score reflects relatively strong engagement in basic management activities, while also highlighting sensitive areas, such as privacy and information search and access, where practices remain less consistent.

Table 4. Levels of Personal Information Management

Personal Information Management (PIM)				
Dimension	Item	Mean	SD	level
Organising	I keep old and new files on the same subject separate from each other	3.49	1.316	Moderate
	I distinguish files that have been completed from those that are still being worked on.	3.87	1.112	High
	I divide my files into folders according to their subject.	4.34	0.945	High
	I am consistent when naming different files on the same topic.	3.90	1.050	High
	I create metadata, headers, or descriptive tag information for my files.	3.49	1.211	Moderate
	I frequently classify the storage locations of my files by reviewing them.	3.79	1.091	High
	By giving the date, sequence number, or version number to new files I create on the same subject, I indicate which one is the most recent.	3.63	1.216	Moderate
	When there is more than one file on the same subject, I can easily see which is the latest version.	3.95	1.042	High
	I create folders in a hierarchical structure.	3.80	1.060	High
	I group applications or programmes on my devices into folders by topic.	3.91	1.047	High
Organising		4.28	0.775	High
Erasing	I delete emails I do not need.	3.41	1.357	Moderate
	I check for and delete duplicate files.	3.91	1.158	High
	I delete files I do not use.	3.83	1.158	High
	I delete backed-up files from my device so that they do not take up space.	3.80	1.208	High
	I delete files I do not need so they do not take up storage.	4.02	1.144	High
	After taking a lot of photos, I check them to avoid taking up too much space and delete photos with shooting errors or poor quality.	3.99	1.183	High
	I erase all the content I do not need so I do not confuse myself.	3.84	1.123	High
	Erasing	3.83	0.978	High
Search-Retrieval	Since I do not store my files regularly, I usually cannot access the file I am looking for.	3.66	1.110	Moderate
	I find it very difficult to access my files without a search box.	3.52	1.311	Moderate
	I lose a lot of time searching for my files.	3.82	1.198	High
	I think it is difficult to archive files.	3.59	1.254	Moderate

	I usually store files randomly because I think it is difficult to archive them.	3.39	1.203	Moderate
	Search-Retrieval	3.59	1.060	Moderate
Privacy	I can access the file I am looking for quickly and easily.	3.87	.949	High
	I encrypt files that I do not want anyone else to access.	3.29	1.270	Moderate
	I pay attention to the privacy of my files.	3.87	1.087	High
	I keep my private files out of other people's reach.	3.96	1.017	High
	Privacy	3.64	0.858	Moderate
Back-Up	I keep a few copies of my files on an external hard drive, in the cloud, or on other devices.	3.83	1.050	High
	I create a backup of the same file in more than one place.	3.46	1.141	Moderate
	I back up my files periodically.	3.93	1.023	High
	Back-Up	3.74	0.924	High
Course Document Management	I regularly archive my notes or documents for my courses.	3.88	1.092	High
	I can access my course-related files quickly when necessary.	3.96	1.031	High
	I classify the photographs, videos, or sound recordings that I take during classes.	3.68	1.197	High
	I think I will be able to use my lecture notes in the future when necessary.	4.13	1.060	High
	Course Document Management	3.90	0.955	High
Digital Literacy	I know how to solve my own technical problems.	3.88	1.007	High
	I can learn new technologies easily.	3.89	1.001	High
	I keep up with important new technologies.	3.93	0.920	High
	I know about many different technologies.	3.74	0.896	High
	I have good ICT skills.	3.80	0.885	High
	Digital Literacy	3.84	0.826	High
	Overall PIM	3.79	0.702	High

*Note: 1 = Never; 2 = Rarely; 3 = Sometimes; 4 = Often; 5 = Always

Students reported using digital platforms such as Microsoft OneNote, Mendeley, and Zotero to support academic work, which contributes to their engagement with information management. However, the interview findings also reveal difficulties in deciding what information should be retained. HAG10 described using Mendeley and Zotero for research and Microsoft OneNote for personal notes, while LAG01 reported uncertainty about which files should be backed up because most files appeared important. These findings indicate that having digital tools does not necessarily result in systematic PIM; tool availability can support organisation, while the absence of selection and retention criteria can contribute to accumulation. To illustrate, the interview participants stated:

"I generally use Mendeley and Zotero for research. I keep my personal notes in Microsoft OneNote." (HAG10)

"I often don't know which files to back up; most of them seem important to me. I don't check them regularly once they're backed up." (LAG01)

"But sometimes it's difficult to decide which data is important to me; all information seems important." (LAG07)

Activities connected to privacy ($M = 3.64$, $SD = 0.858$) and information search and access ($M = 3.59$, $SD = 1.060$) are categorised as moderate. Within privacy, students reported paying attention to privacy ($M = 3.87$, $SD = 1.087$) and keeping private files away from others ($M = 3.96$, $SD = 1.017$), whereas file encryption was lower ($M = 3.29$, $SD = 1.270$). This difference indicates that students tend to rely more on behavioural or access-based protection than on technical protection. Similarly, in information search and access, students reported losing considerable time searching for files ($M = 3.82$) and having trouble accessing files without a search box ($M = 3.52$). Thus, the moderate dimension scores reflect differences between basic privacy and retrieval practices and more advanced forms of control.

Students reported using security features such as tiered access, multifactor authentication, and password protection when exchanging documents, indicating an understanding of privacy as access control. However, the survey item on file encryption was comparatively low ($M = 3.29$, $SD = 1.270$), and HAG08 explicitly described using access levels, passwords, and multifactor authentication *“not data encryption, auditing, etc”*. This convergence of survey and interview findings indicates that students are familiar with accessible security controls but less likely to incorporate advanced technical safeguards into routine PIM.

“I enable security features that are confidential or private to relevant people only, limited to levelled access, passwords, and multifactor authentication, not data encryption, auditing, etc” (HAG08)

In terms of information search and access, the survey indicates inconsistent retrieval practices. The interviews clarify why these difficulties can coexist with effective digital search tools. LAG01 explained that files become mixed because of inconsistent organisation, while LAG06 reported that the computer search function makes retrieval easy but also noted, *“Sometimes I download the same file 10 times or even more.”* Thus, search technology can compensate for weak organisation in the short term, but repeated downloading may also indicate duplication and limited control over the information collection.

“It is difficult, but files related to my interests are easy to find. Because I am inconsistent, my files get mixed up” (LAG01)

Overall, the survey and interview findings indicate that students possess practical digital skills and engage actively in PIM, but their practices are not equally systematic across activities. Basic organisation, course document management, and routine backup are relatively well established, whereas encryption, structured deletion, descriptive metadata, and consistent retrieval require further development. PIM therefore appears to be shaped partly by immediate academic and practical demands rather than by a fully integrated, sustained management strategy.

iii. The relationship between IPA and PIM among students

The Spearman rank correlation showed a statistically significant positive association between Information Privacy Awareness and Personal Information Management ($p = .709$, $p < .001$, $N = 136$). This indicates that students who reported higher levels of privacy awareness also tended to report more developed PIM practices. However, the result should not be interpreted as evidence that privacy awareness directly causes better PIM. Rather, the association suggests that awareness and practice are related components of students' information behaviour, while the interview findings help explain the conditions under which awareness is translated into action.

Table 5. Analysis of the relationship between IPA and PIM among students

			Information Privacy Awareness (IPA)	Personal Information Management (PIM)
Spearman's rho	Information Privacy Awareness (IPA)	Correlation Coefficient	1.000	.709**
		Sig. (2-tailed)	.	.000
		N	136	136
	Personal Information Management (PIM)	Correlation Coefficient	.709**	1.000
		Sig. (2-tailed)	.000	.
		N	136	136

** . Correlation is significant at the 0.01 level (2-tailed).

The interview findings provide a practical explanation for the positive association observed in the survey. LAG02 described becoming more cautious after personal experiences, while LAG06 connected privacy awareness with avoiding unofficial or cracked applications because of perceived security risks. HAG03 similarly described choosing safer, trusted platforms and limiting access to personal data. These accounts illustrate how awareness can provide a practical basis for decisions about platforms, access, and information sharing. At the same time, the interviews show that awareness does not automatically produce consistent behaviour, because convenience, technical knowledge, and immediate academic needs can affect implementation.

Taken together, the survey and interview findings suggest that privacy awareness may provide an important cognitive basis for PIM, but awareness alone does not ensure sustained implementation. Students who recognise privacy risks may still use relatively simple organisational and security strategies, particularly when more advanced measures require additional technical knowledge or effort. The relationship between IPA and PIM is therefore best understood as positive but conditional: awareness is associated with management practices, while contextual and practical factors shape how consistently those practices are applied.

"I used to be careless with my personal data, but now I am more cautious, though not always consistent, about sharing personal data, information, and documents. Experiences have motivated me to be more mindful" (LAG02)

"It is related; being more aware of information privacy makes me avoid using illegal or cracked apps because they pose risks to security and data breaches. So, I am trying to use official apps to protect my information recently" (LAG06)

"The rise of doxing, identity theft, and cyberattacks has made me more aware that information on the internet can be misused. That is why I need to control and manage my personal information more by choosing safer, official, trusted platforms and by limiting access to my personal data on my devices" (HAG03)

“Privacy awareness helps establish control when sharing information, installing apps, opening emails, or clicking on other links to avoid viruses that damage or delete data” (HAG04)

However, the qualitative data also demonstrates that this association between IPA and PIM is not entirely consistent across individual experiences. Participants with similar awareness levels did not always report identical practices, particularly in relation to cookies, encryption, backup routines, and social media disclosure. This variation indicates that the correlation captures an overall pattern across the sample rather than a deterministic relationship for every student.

Students’ personal information management practices are indicative of their level of awareness regarding information privacy

A comparison of the High Awareness Group (HAG) and Low Awareness Group (LAG) was conducted to examine how students' personal information management practices reflect their information privacy awareness. The results indicate that both groups regularly manage their digital data for academic and professional reasons, despite differences in awareness levels. This suggests that privacy awareness is shaped not only by conceptual understanding but also by situational risks and functional needs.

While students with higher levels of awareness generally demonstrate good organisational and security practices, several participants reported inconsistent application of their knowledge in daily life. Other participants showed varying levels of engagement inconsistency, and some appeared to deliberately disengage from developing greater privacy awareness.

“Knowledge gained through education and reading has helped shape my awareness of privacy. As a result, I regularly manage my personal information by avoiding unofficial platforms and using incognito mode when visiting certain websites that require accepting cookies or similar technologies” (HAG04)

“My usual practice is to accept all cookies without understanding or looking into their functions, because the settings are complicated and I want to access the sites I need more quickly” (LAG10)

The LAG interviews typically describe a more reactive form of privacy awareness, in which concerns emerge after media exposure or personal experiences with security risks. For example, LAG05 reported that automated backup was available but not consistently monitored, while LAG10 explained that cookies were often accepted because the settings were complicated and quick access was prioritised. These accounts suggest that convenience and immediate functionality can compete with privacy-protective practices. Rather than treating this pattern as a uniform “privacy paradox”, the findings indicate a context-dependent tension between privacy protection, accessibility, and self-presentation.

“I set up automated backups on the device. However, the main challenges are that it is not yet a priority and monitoring is inconsistent, so it is quite difficult to find information. So far, I just heard from media” (LAG05)

“I usually accept all cookies without understanding or looking into their functions because the settings are complicated and to access the needed sites more quickly. Even if sharing data is important, personal brand is also needed” (LAG10)

HAG, in contrast, more often described proactive privacy practices supported by information-seeking, training, and formal instruction. HAG05 emphasised the importance of structured information management for retrieval, while HAG08 reported attention to privacy settings, document access, location permissions, and two-factor authentication. These practices illustrate how higher awareness can be accompanied by a broader repertoire of protective actions. Nevertheless, even among HAG participants, the findings indicate that systematic management is not complete and that manual organisation and retrieval remain important parts of their workflows.

“Well-organised and structured information management is crucial, especially for the ease of retrieving information. Maybe still done manually but important to know well our documents” (HAG05)

“Control is definitely necessary when managing and sharing information; I restrict my use of social media to avoid risks” (HAG06)

“Maintaining one's privacy helps prevent risks that could endanger oneself or others, in addition to influencing one's management practices. I've been taking part in educational programmes” (HAG07)

“I pay attention to security settings such as privacy on social media, document access across various apps, location access, or even using two-factor authentication” (HAG08)

Overall, students in both groups possess the basic understanding required to effectively manage personal information and reduce digital risks. The comparison highlights a gap between awareness and integrated practice. The HAG accounts generally describe a broader range of protective and organisational strategies, whereas LAG accounts more often emphasise convenience, immediate academic needs, or reactive responses. The contrast therefore concerns not simply whether students are aware of privacy, but how that awareness is incorporated into everyday information-management routines.

Thus, the findings indicate a positive but conditional relationship between privacy awareness and PIM, together with variation in implementation. Privacy awareness appears to support privacy-protective and organisational behaviour, but it does not guarantee consistent adoption of technically demanding or routine practices. This distinction is important for interpreting the strong correlation without making a causal claim.

DISCUSSION

The survey and interview findings indicate that Indonesian postgraduate students in Türkiye demonstrate a high overall level of information privacy awareness, although the dimensions of attention, security, and communication are not equally developed. Attention was particularly strong, whereas security and communication were moderate. Item-level and interview evidence suggests that students are more comfortable with basic privacy-protective behaviours than with technically demanding practices such as encryption and detailed cookie management. Communication practices are also shaped by academic, professional, and self-presentation needs. Meanwhile, some students have disregarded the privacy settings on local mobile apps for the sake of convenience, ignored security warnings on public websites due to language barriers, and used unprotected public Wi-Fi for sensitive transactions, among other things. These findings are consistent with the broader

observation that recognising the importance of privacy does not necessarily translate into equally consistent everyday practices. This statement is consistent with Eroğlu's (2018) observation that students do not always apply their knowledge of personal data rights and protection in practice. Their understanding of privacy remains largely conceptual, viewing it as a form of social control, which contributes to the gap between awareness and behaviour.

The reality faced by Indonesian students also reflects strategies for adaptation within a cross-cultural environment. Students are required to interact with the digital ecosystem of local educational institutions, cross-border communication networks, and local administrative platforms, whilst working within existing limitations. The transition to a cross-cultural academic and digital ecosystem requires international students to navigate unfamiliar institutional platforms, local digital administrative infrastructure (such as university portals and national digital services), and compliance with foreign data governance frameworks such as the Turkish Personal Data Protection Act alongside the Personal Data Protection Act. International students often experience increased vulnerability in foreign digital spaces due to language barriers and unfamiliarity with local privacy policies, which paradoxically heightens their general awareness of privacy risks whilst simultaneously hindering their ability to implement advanced technical safeguards. Consequently, due to a lack of control over technical capabilities such as cookie management, security certification, encryption methods, information organisation, deletion, and access, students may find it difficult to use digital content efficiently and securely in the long term (Koçak, 2021).

The findings also have implications for PIM practice. Data security techniques can reduce information-management difficulties when they are integrated into everyday routines, but the present results indicate that students still rely heavily on basic access controls, passwords, search functions, and manually organised folders. This aligns with the view expressed by Külcü and Henkoğlu (2014, p. 232) that effective digital information management is a method of protecting personal data that relies on the behaviour of informed data owners. In practice, students rely heavily on third-party cloud storage to manage various documents without a structured folder system. Even students reporting higher awareness may experience difficulties with retrieval, duplication, or the integration of multiple platforms. This means they prioritise rapid retrieval and accessibility over systematic security to cope with the cognitive load involved in managing documents across platforms and borders. Consequently, students experience reduced system reliability, a loss of control due to information overload, problems with time management, difficulties in decision-making, and inefficient use of resources (Knippenberg et al., 2015). This can even lead to emotional and cognitive decline within their data ecology.

Accordingly, practice-oriented support may be more useful than awareness-raising alone, particularly when it develops concrete skills in secure file management, encryption, access control, retention and deletion, and systematic organisation. High scores for attention to detail and subject-based folder organisation reflect an urgent need for self-protection to ensure that academic documents remain organised. However, the low uptake of encryption and the high incidence of document duplication suggest that studying abroad often leads to reactive management practices aimed at saving time and ensuring convenience, rather than the implementation of a systematic data lifecycle. Information organisation practices, such as procedures for collecting, storing, organising, and sharing personal data, are also shaped by variations in experience, habits, culture, language, academic background, and life experiences in dealing with uncertainty (Fatima et al., 2019, p. 7; Gao, 2023). Factors including cross-cultural encounters and personal adaptation to new environments can

influence how information awareness and practices develop in a global context (Krtalić & Alon, 2024).

The significant positive association between IPA and PIM provides evidence that students with higher reported privacy awareness also tend to report more developed information-management practices. However, the interview findings qualify this relationship. Students described differences in organisation, deletion, retrieval, backup, encryption, and information sharing even when their general awareness was relatively high. Converting conceptual understanding into consistent practices of collecting, storing, organising, and sharing personal information therefore remains challenging. For international students, these practices occur across academic, social, and transnational information environments, where language, cultural experience, academic demands, and access to digital services may shape information behaviour. The present findings consequently suggest an association between awareness and practice rather than a deterministic pathway from one to the other.

Although privacy awareness serves as a strong cognitive foundation as seen in the HAG, who proactively avoid pirated applications and manage location permissions – factors such as cognitive load and limited technical knowledge often undermine these intentions. When faced with tight academic deadlines whilst studying abroad, students tend to adopt functional shortcuts; for example, ignoring complex cookie settings or using simple passwords rather than advanced encryption. This demonstrates that awareness does not automatically translate into consistent behaviour without the support of operational ease.

The comparison between the HAG and LAG further illustrates this conditional relationship. HAG participants more frequently described proactive information-seeking, training, and multiple protective strategies, whereas LAG participants more often described reactive responses to privacy risks and a stronger emphasis on convenience. According to Zhang et al. (2014) and Kani-Zabihi and Helmhout (2012), LA group behaviour reflects actions that contribute to privacy violations, such as a lack of awareness regarding information security, accepting privacy policies without reading them carefully, or a lack of awareness of legal regulations. These patterns reflect the persistence of the privacy paradox, whereby individuals' express concerns about privacy whilst simultaneously engaging in behaviour that may increase privacy risks. These differences are visible in interview accounts concerning cookies, automated backups, social media use, and organisation. At the same time, the HAG findings also show that higher awareness does not eliminate practical difficulties in integrating platforms, devices, and routines. These challenges are compounded by the psychological and logistical burdens of living abroad, where reliance on informal peer networks for safety advice sometimes leaves them exposed to unverified practices.

The findings of this study confirm a widespread phenomenon in the digital privacy literature concerning the gap between awareness and actual protective behaviour. However, this study makes an original contribution by demonstrating how these dynamics manifest themselves in a unique way among a group of Indonesian postgraduate students studying in Türkiye. In contrast to students studying in their homeland – where the digital environment is relatively homogeneous – Indonesian students find themselves at the crossroads of dual digital identities: maintaining professional or personal networks in Indonesia whilst simultaneously building their reputation and academic networks there. For international students, the language barrier in understanding the terms and conditions of local platforms, alongside cross-border academic pressures, increases the potential for inconsistencies in behaviour.

In theoretical terms, this study expands the literature by arguing that the correlation between privacy awareness and PIM is conditional, being significantly influenced by external contextual variables. Awareness is an important component of information behaviour, but its translation into practice depends on technical skills, convenience, academic demands, and social or professional contexts. Educational interventions may therefore benefit from moving beyond general awareness towards applied skills in secure file management, encryption, systematic organisation, retrieval, and responsible information sharing. Such an approach would address the observed gap between recognising privacy risks and incorporating privacy-protective practices into everyday academic and digital routines.

CONCLUSION

This study shows that Indonesian postgraduate students in Türkiye have a high overall level of privacy awareness, which is positively associated with their personal information management practices. However, the relationship between awareness and practice is uneven, as students who recognise the importance of privacy do not necessarily apply protective measures consistently in their academic and everyday digital routines. Students demonstrate greater proficiency in basic privacy-protective behaviours than in technically demanding practices such as encryption and detailed cookie management, while many of their practices remain reactive and are shaped by convenience, academic demands, and professional or social contexts. Furthermore, the comparison between groups suggests that higher awareness is associated with broader and more consistent practices, but not with the removal of practical difficulties. Educational interventions should therefore move beyond awareness-raising towards applied skills in secure file management, encryption, access control, retention and deletion, retrieval, and responsible information sharing.

ACKNOWLEDGMENTS

The authors sincerely thank all contributors to this study, especially Indonesian postgraduate students across Türkiye who participated as respondents. Appreciation is also extended to the Turkish Scholarship for its support and facilities throughout this research. The authors acknowledge the use of DeepL (free version) to improve the clarity and grammar of the manuscript, and Napkin AI to assist in organising and presenting qualitative thematic findings. All outputs were reviewed and verified by the authors, who remain fully responsible for the content in accordance with COPE and journal ethical standards.

CONFLICT OF INTEREST

The authors have no relevant competing interests to declare.

ETHICAL APPROVAL AND INFORMED CONSENT STATEMENTS

This study was approved by the Hacettepe University Ethics Committee for Social Sciences and Humanities Research under reference number E-66777842-300-00004089928 on 25 February 2025. All participants provided informed consent after receiving an explanation prior to participation, and their confidentiality and anonymity were strictly maintained in accordance with applicable ethical guidelines.

AUTHOR CONTRIBUTIONS

Conceptualization: [Nurthoyyibah, M. S.]; Methodology: [Nurthoyyibah, M. S. and Külcü, Ö.]; Formal analysis and investigation: [Nurthoyyibah, M. S. and Külcü, Ö.]; Writing - original draft preparation: [Nurthoyyibah, M. S.]; Writing - review and editing: [Nurthoyyibah, M. S. and Külcü, Ö.].

REFERENCES

- Barreau, D. K. (1995). Context as a factor in personal information management systems. *Journal of the American Society for Information Science*, 46(5), 327–339. [https://doi.org/10.1002/\(SICI\)1097-4571\(199506\)46:5<327::AID-ASIA4>3.0.CO;2-C](https://doi.org/10.1002/(SICI)1097-4571(199506)46:5<327::AID-ASIA4>3.0.CO;2-C)
- Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology: Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 57–71). American Psychological Association. <https://doi.org/10.1037/13620-004>
- Chaudhry, A. S., & Alajmi, B. M. (2024). Personal information management practices: How scientists find and organize information. *Global Knowledge, Memory and Communication*, 73(6–7), 757–774. <https://doi.org/10.1108/GKMC-04-2022-0082>
- Choi, H. S., Lee, W. S., & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modeling. *Computers & Security*, 67, 244–253. <https://doi.org/10.1016/j.cose.2017.03.007>
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). SAGE Publications.
- Detlor, B. (2010). Information management. *International Journal of Information Management*, 30(2), 103–108. <https://doi.org/10.1016/j.ijinfomgt.2009.12.001>
- Eroğlu, Ş. (2018). Dijital yaşamda mahremiyet (gizlilik) kavramı ve kişisel veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 35(2), 130–153. <https://doi.org/10.32600/huefd.439007>
- Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., & Yasin, A. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, 48, Article 102351. <https://doi.org/10.1016/j.jisa.2019.06.007>
- Gao, H. (2023). Transnational habitus as a configuration of dispositions: Chinese international students navigating online information. *Literacy Research: Theory, Method, and Practice*, 72, 139–160. <https://doi.org/10.1177/23813377231176259>
- Heading, S., & Cavaciuti-Wishart, E. (2024, January 10). These are the biggest global risks we face in 2024 and beyond. *World Economic Forum*. <https://www.weforum.org/agenda/2024/01/global-risks-report-2024/>
- Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25(1), 1–24. <https://doi.org/10.1080/07370020903586662>
- Jones, W., & Teevan, J. (Eds.). (2007). *Personal information management*. University of Washington Press.
- Kani-Zabihi, E., & Helmhout, M. (2012). Increasing service users' privacy awareness by introducing on-line interactive privacy features. In P. Laud (Ed.), *Information security technology for applications* (pp. 131–148). Springer. https://doi.org/10.1007/978-3-642-29615-4_10

- Koçak, O. (2021). Development and validation of a scale for assessing personal digital content management skills of higher education students. *Malaysian Journal of Library and Information Science*, 26(2), 69–87. <https://doi.org/10.22452/mjlis.vol26no2.4>
- Korkmaz, Ö., Vergili, M., & Karadaş, E. (2021). Developing online privacy awareness scale: Reliability and validity study. *Türkiye Bilimsel Araştırmalar Dergisi*, 6(2), 297–311.
- Krtalić, M., & Alon, L. (2024). Personal cultural heritage management: A conceptual framework for constructing and curating cultural identities through personal collections. *Journal of Documentation*, 80 (6), 1238–1257. <https://doi.org/10.1108/JD-02-2024-0043>
- Krtalić, M., & Ihejirika, K. T. (2022). The things we carry: Migrants' personal collection management and use. *Journal of Documentation*, 79(1), 86–111. <https://doi.org/10.1108/JD-12-2021-0236>
- Külcü, Ö., & Henkoğlu, T. (2014). Sosyal paylaşım ağlarında gizlilik: Facebook incelemesi. *Bilgi Dünyası*, 15(2), 231–252. <https://doi.org/10.15612/BD.2014.424>
- Sharma, S. K., Mudgal, S. K., Gaur, R., Chaturvedi, J., Rulaniya, S., & Sharma, P. (2024). Navigating sample size estimation for qualitative research. *Journal of Medical Evidence*, 5(2), 133–139. https://doi.org/10.4103/jme.jme_59_24
- Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. L. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), 459–468. <https://doi.org/10.1037/0021-9010.68.3.459>
- van Knippenberg, D., Dahlander, L., Haas, M. R., & George, G. (2015). Information, attention, and decision making. *Academy of Management Journal*, 58(3), 649–657. <https://doi.org/10.5465/amj.2015.4003>
- Youm, S., Han, C., Yoo, H., Jang, S. H., & Dorr, B. J. (2026). “I still need your help”: Online information seeking behavior of international students in the United States on Reddit. *PLOS ONE*, 21(2), Article e0341314. <https://doi.org/10.1371/journal.pone.0341314>
- Zhang, B., Wang, N., & Jin, H. (2014). Privacy concerns in online recommender systems: Influences of control and user data input. In *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS 2014)* (pp. 159–173). USENIX Association.

Appendix 1: Survey instrument

Items for Information Privacy Awareness (Korkmaz et al, 2021)	Loadings	Cronbach's Alpha
Attention		0.920
I check the privacy settings and notifications of the online platforms I use.	0.826	
I set the privacy settings for my accounts on the online platforms I use (social networks, shopping sites, games, etc.).	0.783	
I make sure the passwords I use online are strong (using upper-case and lower-case letters, numbers, special characters, and at least eight characters).	0.723	
I can tell whether the content of messages I receive by email or on social media is reliable.	0.776	
I understand whether messages or emails from people I do not know in online environments pose a security risk.	0.758	
Information I share online may be accessed by companies, government agencies, or hackers.	0.748	
I am aware that the information I share on online platforms may be used by malicious individuals.	0.746	
Security		0.857
I am aware of the cookies used by websites.	0.574	
When installing an app on my mobile device, I pay attention to the permissions it requests.	0.672	
I check the security certificates and data encryption methods of websites and mobile applications.	0.555	
I check the security of the websites I visit.	0.721	
I pay attention to what information browser extensions will access.	0.694	
Communication		0.771
I share my personal information (address, date of birth, age, occupation, phone number, etc.) with people I do not know in online environments.	0.688	
I share screenshots of my conversations with friends or relatives without asking for permission.	0.829	
I share information, pictures, videos, and other content belonging to others online without asking for permission	0.827	
I allow people I do not know to follow me or add me as a friend online.	0.672	
I communicate with people I do not know in online environments.	0.583	
Item for Personal Information Management (Koçak, 2021)	Loadings	Cronbach's Alpha
Organising		0.913
I keep old and new files on the same subject separate from each other	0.561	
I distinguish files that have been completed from those that are still being worked on.	0.701	
I divide my files into folders according to their subject.	0.748	
I am consistent when naming different files on the same topic.	0.790	
I create metadata, headers, or descriptive tag information for my files.	0.593	
I frequently classify the storage locations of my files by reviewing them.	0.689	
By giving the date, sequence number, or version number to new files I create on the same subject, I indicate which one is the most recent.	0.678	
When there is more than one file on the same subject, I can easily see which is the latest version.	0.771	
I create folders in a hierarchical structure.	0.728	

I group applications or programmes on my devices into folders by topic.	0.630	
Erasing		0.919
I delete emails I do not need.	0.517	
I check for and delete duplicate files.	0.622	
I delete files I do not use.	0.692	
I delete backed-up files from my device so that they do not take up space.	0.650	
I delete files I do not need so they do not take up storage.	0.614	
After taking a lot of photos, I check them to avoid taking up too much space and delete photos with shooting errors or poor quality.	0.624	
I erase all the content I do not need so I do not confuse myself.	0.611	
Search-Retrieval		0.921
Since I do not store my files regularly, I usually cannot access the file I am looking for.	0.886	
I find it very difficult to access my files without a search box.	0.876	
I lose a lot of time searching for my files.	0.905	
I think it is difficult to archive files.	0.845	
I usually store files randomly because I think it is difficult to archive them.	0.855	
Privacy		0.829
I can access the file I am looking for quickly and easily.	0.774	
I encrypt files that I do not want anyone else to access	0.532	
I pay attention to the privacy of my files.	0.675	
I keep my private files out of other people's reach.	0.610	
Back-Up		0.827
I keep a few copies of my files on an external hard drive, in the cloud, or on other devices.	0.760	
I create a backup of the same file in more than one place.	0.611	
I back up my files periodically.	0.694	
Course Document Management		0.893
I regularly archive my notes or documents for my courses.	0.738	
I can access my course-related files quickly when necessary.	0.760	
I classify the photographs, videos, or sound recordings that I take during classes.	0.663	
I think I will be able to use my lecture notes in the future when necessary.	0.679	
Digital Literacy		0.924
I know how to solve my own technical problems.	0.703	
I can learn new technologies easily.	0.651	
I keep up with important new technologies.	0.653	
I know about many different technologies.	0.565	
I have good ICT skills	0.585	