Received 5 January 2022
Revised 5 May 2022
1 August 2022
Accepted 30 September 2022

The influence of ethical principles and policy awareness priming on university students' judgements about ICT code of conduct compliance

Deborah Richards and Salma Banu Nazeer Khan
School of Computing, Macquarie University, Sydney, Australia
Paul Formosa
Department of Philosophy, Macquarie University, Sydney, Australia, and
Sarah Bankins
Department of Management, Macquarie University, Sydney, Australia

Abstract

Purpose – To protect information and communication technology (ICT) infrastructure and resources against poor cyber hygiene behaviours, organisations commonly require internal users to confirm they will abide by an ICT Code of Conduct. Before commencing enrolment, university students sign ICT policies, however, individuals can ignore or act contrary to these policies. This study aims to evaluate whether students can apply ICT Codes of Conduct and explores viable approaches for ensuring that students understand how to act ethically and in accordance with such codes.

Design/methodology/approach – The authors designed a between-subjects experiment involving 260 students' responses to five scenario-pairs that involve breach/non-breach of a university's ICT policy following a priming intervention to heighten awareness of ICT policy or relevant ethical principles, with a control group receiving no priming.

Findings – This study found a significant difference in students' responses to the breach versus non-breach cases, indicating their ability to apply the ICT Code of Conduct. Qualitative comments revealed the priming materials influenced their reasoning.

Research limitations/implications – The authors' priming interventions were inadequate for improving breach recognition compared to the control group. More nuanced and targeted priming interventions are suggested for future studies.

Practical implications – Appropriate application of ICT Code of Conduct can be measured by collecting student/employee responses to breach/non-breach scenario pairs based on the Code and embedded with ethical principles.

Social implications – Shared awareness and protection of ICT resources.

Originality/value – Compliance with ICT Codes of Conduct by students is under-investigated. This study shows that code-based scenarios can measure understanding and suggest that targeted priming might offer a non-resource intensive training approach.

Keywords Information communication technology code of conduct, Cyberethical scenarios, AI4People ethical principles, Moral sensitivity, Priming

Paper type Research paper

This work is supported by a Macquarie University MRes Year 2 Scholarship to the second author and an Australian Research Council Discovery Grant: DP200102131 - Cybersecurity ethics training simulations for values-based decision-making.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 2, 2022
pp. 134-161
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-01-2022-0001

1. Introduction

Advanced computing technologies bring risks of unethical cyber hygiene practices and cybersecurity threats to individuals and organisations (Vallor and Rewak, 2018). To mitigate these threats, most organisations require users of their information and communication technology (ICT) resources to agree to an ICT Code of Conduct. In the case of universities, agreeing to abide by the ICT Code of Conduct is typically one of several agreements signed prior to enrolment by new students. An ICT Code of Conduct refers to the "rights, duties and responsibilities of technology users" (Bia and Kalika, 2007, p. 3) and includes guidelines and policies around the safe, ethical and efficient use of organisational IT infrastructure. Adoption of these codes is impacted by factors such as organisational structure, standards, technologies and size (Bia and Kalika, 2007). Nonetheless, individuals often ignore or violate such policies and behave unethically in their use of ICT resources (Leonard and Cronan, 2005). This poses significant risks to individuals, such as through insecurity of their data, and significant cybersecurity risks for organisations that can impact their reputational and financial standing. Such non-adherence may be due to many younger ICT users not being mindful of cyber safety or good cyber hygiene practices (Smith, 2018; Cain *et al.*, 2018). Further, ICT policy compliance can also depend on the relevant ethical values, sensitivities and knowledge of individuals about what constitutes ethical ICT usage (Vallor and Rewak, 2018).

To help motivate ICT compliance, students need more education around cybersecurity risks (Snyder, 2004), the content of ICT policies, the importance of intellectual property rights (Kruger, 2003), and the ethical foundations of ICT and cybersecurity policies (Formosa *et al.*, 2021). However, the time required to design and deliver such training necessitates significant organisational commitment and investment of resources to potentially restructure curricula and ensure students from all disciplines receive relevant training. But the current absence of training related to ICT Codes of Conduct in many universities and organisations exposes them to cyber risks.

To identify a potential viable means to raise awareness of cybersecurity risks, we draw inspiration from the literature showing that priming, in which an individual is reminded of a moral code, changes how people think about their own behaviour (Ariely, 2012), and this change can encourage/discourage honest/dishonest behaviour (Mazar *et al.* (2008), including in an information security context (Sharma *et al.*, 2021). We build on this work to examine whether priming individuals toward heightened awareness of either (1) relevant ICT policies or (2) the ethical principles underlying those polices improves their ability to identify cybersecurity breaches, when compared to receiving no priming. Guided by the work of Nyinkeu *et al.* (2018), we present users with realistic cyberethical dilemmas, reflecting breaches of ICT policies and cybersecurity ethical principles, to measure users' ethical sensitivity and the value of priming them to the content of either the ICT Code of Conduct or the ethical principles underpinning those policies, compared to a control group receiving no priming. In the following section, we review related literature and develop our research questions. Section 3 presents our methodology, followed by results in Section 4. Section 5 discusses the results and responds to the research questions. Conclusions and future research directions are provided in Section 6.

2. Background literature and research questions

Cybersecurity policies can impose ethical obligations on individuals to use their organisations' ICT infrastructure safely. Users' understanding of the ethical foundations of such policies can help to mitigate cybersecurity challenges and reduce the potential for security breaches (Vallor and Rewak, 2018). To promote ethical behaviour, professional bodies such as the Association for Computing Machinery (ACM) and Institute of Electrical

and Electronics Engineers (IEEE) have codes of ethics which members must uphold. Such profession-based norms have a positive effect on users' sense of obligation to maintain such codes and their consequent computer security behaviour (Yoon and Kim, 2013). This sense of obligation can be promoted by increasing individuals' awareness of their ICT and related ethical responsibilities (Vallor and Rewak, 2018). Students at universities are also subject to ICT policies and are recognised as a particularly vulnerable cohort of users due to a lack of good cyber hygiene practices (Garrison and Posey, 2006; Maennel *et al.*, 2018; Smith, 2018). Introducing better-informed ICT policy as curriculum at the university can boost students' compliance towards usage of ICT resources and improve cybersecurity knowledge (Neigel *et al.*, 2020). It has been identified that university students show more ICT compliance when they receive notifications to threats in response to ICT breaches, as this builds trust towards university notifications (Han *et al.*, 2015). Assisting students in identifying and ethically dealing with cybersecurity challenges, such as protecting ICT assets, is important not only for universities but also for the organisations that students will later join as employees.

Whether individuals practice good cyber hygiene depends on the individual's moral beliefs and behavioural intentions (Vallor and Rewak, 2018; Moody *et al.*, 2018). A unified model of security policy compliance (UMISPC) identifies that an individual's role values (work and task responsibilities), fear (avoiding negative stimulus behaviours) and habit (natural tendency to be compliant) are the important predictors of compliance to information security systems (Moody *et al.*, 2018). Encouraging users to adopt ethical principles in their use of ICT technologies can reduce cyber threats and enhance cyber hygiene practices (Vallor and Rewak, 2018). Ethical principles enable organisations not only to anticipate significant mistakes but also to efficiently mitigate them (Floridi *et al.*, 2018). The organisation's success depends on the effective use of information resources, which must be used to foster individuals' positive attitudes and beliefs toward ICT policy compliance (Cram *et al.*, 2017). While virtue ethics, utilitarianism and deontological ethics are sometimes used to frame the ethical issues around cybersecurity (Manjikian, 2018), in applied ethics a more common approach, especially in an educational context, is the use of principlist frameworks (Formosa *et al.*, 2021). In bioethics, Beauchamp and Childress's (2001) four principles of beneficence (benefiting people), non-maleficence (not harming people), autonomy (allowing choice and consent) and justice (being fair and unbiased) have been widely used. These four principles, along with a fifth principle of explicability (involving intelligibility, transparency and accountability), have been applied to the ethical use of artificial intelligence (AI) through the AI4People Framework (Floridi *et al.*, 2018; Floridi and Cowls, 2019). The five principles from this framework have recently been extended to the context of cybersecurity (Formosa *et al.*, 2021) and have been used as a basis to teach cybersecurity ethics to individuals through a serious videogame (Richards *et al.*, 2020). Given the prevalence of principlist frameworks and their usefulness in a cybersecurity educational context, we adopt this framework and its five ethical principles in our study. We now turn to the development of our two research questions.

2.1 Security awareness and practice of university students

To understand how well students recognise cybersecurity issues and judge risks associated with various ICT behaviours, Yan *et al.* (2018) conducted a scenario-based survey with 462 university students from north-eastern United States public universities. They found that 12% of the 16 scenarios were incorrectly judged by the students, and the judgements of 23% of the students were below 50% accuracy. The study suggests that students were the weakest link in the organisation regarding sound cybersecurity judgements. The survey concluded that accounting students require cyber education and knowledge to support good cyber practices (Yan *et al.*, 2018).

Another survey conducted in Pakistan with 643 students and 378 teachers from four public and private universities showed a lack of knowledge of ethics in IT and strongly

recommended that universities provide awareness training about ethical IT use (Jamil and Shah, 2014). Another study conducted in Islamabad involving 304 participants from four universities showed that while students had a positive attitude towards cybersecurity, they lacked adequate knowledge to use cyber technology safely (Jamal *et al.*, 2016). These two studies focused only on testing the cyber hygiene practices of students generally and did not involve dealing with specific dilemmas related to cybersecurity issues.

A study conducted by Woodward *et al.* (2007, p. 196) to understand students' cyberethics knowledge and their ethical reasoning found that students with a good knowledge of ethics valued ethical reasoning and made ethical IT-related decisions. However, this work and the above studies did not link students' understanding of ethical principles to their cyberethical behaviour. To make this link, we draw together students' obligations to use their university's ICT resources in an acceptable way, the ethical principles underlying cyber hygiene and cybersecurity decision-making, and students documented poor cybersecurity awareness and practices to develop our first research question:

RQ1. How can students' sensitivity to the ethical principles underlying their behaviour towards usage of ICT resources be measured?

2.2 Awareness of cybersecurity ethics

Raj *et al.* (2018) propose that best practices in cybersecurity for institutions should include cyber education guidelines in the educational curriculum. Educating students through a strong curriculum on cyber ethics, cyber hygiene, and cybersecurity effectively increases ethical awareness in this area and changes student behaviour (Yan *et al.*, 2018; Smith, 2018). Universities should strive to educate students about these topics by using different approaches, including the use of real-world examples of cybersecurity ethical issues and realistic scenarios, and by engaging with students offline and outside classroom activities to facilitate cyber education (Nyinkeu *et al.*, 2018).

There have been numerous calls for universities to provide training in cybersecurity ethics to students, academics and other employees (Pólkowski, 2015; Marquardson and Gomillion, 2018). While organisations in general face the threat of ICT and cybersecurity breaches (Moody *et al.*, 2018), it is not feasible to use training designed to ensure paid employees follow company policies as students are not paid employees of a university. It has been recognised that there is a need for training to those who want to become future cybersecurity professionals (Blanken-Webb *et al.*, 2018). Examples of such training include Pournaghshband (2013), who introduced cybersecurity and cyber hygiene concepts whilst teaching programming concepts, and the recent curriculum and MOOC created by the "Constructing an Alliance for Value-driven Cyber-security" (CANVAS) project (https://canvas-project.eu). Some training tools have also been provided for non-ICT students. A gaming teaching tool was designed to educate users on societal online platforms about cyber threats and cyberattacks (Tioh *et al.*, 2019; Nguyen and Bhatia, 2020). To enhance the skills of students with non-technical backgrounds, "Riskio" was designed for participants to play the role of a cyber attacker and defender (Hart *et al.*, 2020, p. 1). The gaming card deck was designed to help players identify cyber threats and practice good cyber hygiene (Hart *et al.*, 2020). To educate students about cybersecurity and change their behavioural intentions, Alqahtani and Kavakli-Thorne (2020) also took a gamification approach and created the CybAR app. The findings revealed students' acceptance of games to learn about cybersecurity awareness influenced their "behavioural intentions" (Alqahtani and Kavakli-Thorne, 2020, p. 27). Another recent serious game to teach cybersecurity ethics based on Ryan *et al.* (2017) has been developed by Richards *et al.* (2020) but not yet evaluated.

While initiatives to develop a cyberscience curriculum containing ethics exist, such as the ACM's Cyber Education Project (Richards and Ekstrom, 2015), concerns remain since ethical

decision-making is often minimal or missing from the curriculum and is not provided to all students (Mead *et al.*, 2015). Some advocates, such as Sobiesk *et al.* (2015) and Dupuis (2017), recommend compulsory education in cyber hygiene education for all students; however, Neigel *et al.* (2020) suggest this approach may not be feasible or enforceable across an institution. Comprehensive institution-wide approaches to cyber ethics training are lacking. Another issue concerns the timing of training. Kim (2013) conducted a study in a business college comparing students who had training on information security (IS) with students who learned these concepts from their friends, at work or in class, and concluded that cybersecurity training should be provided at the beginning of the semester to help students practice cyber hygiene and monitor their cyber activities regularly. Finally, the content of the training is an open question. McNamara *et al.* (2018) conducted a study where one group (34 students and 56 professionals) was given a brief introduction to the company's ethical standards, and the other group (29 students and 49 professionals) was given a link to the ACM Code of ethics prior to responding to 11 ethical vignettes. The students who spent at least 30 s reading the ACM Codes of Ethics were the training group. Not surprisingly, since 30 s is a negligible training duration, the study found no significant difference between the two groups (McNamara *et al.*, 2018). There was also no control group (i.e. no ethical sensitisation activity), so it is not possible to see whether both forms of "priming" had been equally successful or inadequate. If the priming had not changed ethical behaviour compared to a control group, it raises the question of how much or what type of training is required to have a significant impact on ethical cyber behaviours.

In the past, there has been some interest in improving students' understanding of their institutional ICT Code of Conduct (Healy and Iles, 2002) to address students' cybercrimes (Sembok, 2004). Healy and Iles (2002) note that two decades ago, institutions adopted different ways to provide information related to ICT ethical issues to students, such as displaying information in computing laboratories and a university's intranet and handbooks. Similarly, Snyder (2004, p. 4) suggested educating students about ICT policy terminologies, discussing the consequences of breaching the policy, and helping them to practice good cyber behaviour to become responsible "cyber-citizens". Despite the current use of ICT codes of conduct as central to ensuring appropriate and ethical use of university ICT resources, since these early studies were conducted, little research has directly explored ICT codes of conduct and student cybersecurity behaviour.

Training students by providing cybersecurity ethical education, creating awareness of ICT policies, and increasing good cyber ethical behaviour remain a pivotal challenge for universities. To our knowledge, educational institutions do not provide all students with training concerning ICT Codes of Conduct. This is in stark contrast to another area concerning potential student misconduct, that of academic integrity, where significant research and extensive resources have been invested to address the problem of academic integrity in educational institutions. Even with mandatory educational modules at many institutions, problems persist globally in academic integrity (Denisova-Schmidt, 2018). In reviewing the efficacy of the multitude of interventions and training programs in academic integrity, Sefcik *et al.* (2019) note a lack of focus on values and consequences of misconduct. Zhang *et al.* (2021) see the greatest issue as a lack of awareness and suggest the use of an academic integrity awareness index. This body of research suggests focussing on the ethical values underlying codes of conduct may be helpful in an educational context. Thus, we seek to follow that advice in exploring training students about appropriate ICT conduct.

Faced with the reality of few resources and minimal institutional focus on compliance with ICT Codes of Conduct, despite the potential for harm, and building on findings from adjacent areas of research, we consider whether a lightweight (i.e. non-resource intensive) approach involving sensitisation or "priming" could be effective in changing behaviour in this area. Priming refers to "an improvement in performance in a perceptual or cognitive task, relative

to an appropriate baseline, produced by context or prior experience" (McNamara, 2005). This involves a "prime", or some type of stimulus that impacts knowledge activation, and a "target", or something that the prime is directed toward influencing (Minton *et al.*, 2017, p. 310). Dual-process theory suggests that individuals process information and form judgements, including moral judgements (Kvaran *et al.*, 2013), through both an unconscious and automatic pathway often based on emotion and intuition (system 1) and a slower, more conscious, deliberate and considered pathway (system 2) (Sharma *et al.*, 2021). Although system 1 thinking may be appropriate for routine information system uses, such as email checking, it is likely to be inadequate for dealing with the more complex issues associated with cybersecurity threats (Sharma *et al.* (2021). Priming can be used to disrupt system 1 thinking and prompt individuals to activate system 2 thinking, thus heightening the likelihood that they will respond appropriately to, for example, cybersecurity risks they might be facing (Sharma *et al.*, 2021). Empirical work is emerging to support this logic, with evidence that priming interventions can reduce risky behaviour related to information security (Sharma *et al.*, 2021), that priming individuals with the negative outcomes of risky behaviours can prompt safer cybersecurity choices (Rosoff *et al.*, 2013), and that "risk priming" can momentarily affect users' security update decisions (Shieh and Rajivan, 2021). However, there is also evidence that priming may be ineffective against more sophisticated forms of cyberattacks (Junger *et al.*, 2017). These competing findings suggest that more research is required to understand the contexts in which priming is effective for encouraging cyber ethical behaviour.

To contribute to this area of research in a specific context, we focus on priming to increase students' awareness of and compliance with ICT codes of conduct to encourage better cybersecurity ethical judgements. Specifically, we explore whether being reminded of the ICT policy itself or being exposed to the underlying ethical principles informing such a policy are effective for encouraging ethical behaviour when compared to no priming being provided. This leads to our second research question:

RQ2. Does priming students about (1) an ICT Code of Conduct or (2) relevant ethical principles influence their judgements about ICT policy compliance?

3. Methodology

A mixed-method approach was employed to address the research questions. We used the experimental vignettes methodology (EVM) (Aguinis and Bradley, 2014), an extensively used survey technique requiring participants to make "explicit decisions, judgments, and choices or express behavioural preferences" (Aguinis and Bradley, 2014, p. 354). The EVM allowed us to assess participants' willingness to make ethical decisions following their university's ICT policy. A quantitative, between-subjects experiment examined participants' responses to five scenarios representing breach/non-breach of a university's ICT policy, following different priming interventions. Following their scenario responses, participants were invited to provide qualitative open-ended responses to allow deeper interrogation of how they approached the scenarios. A between-subjects design is suitable for our study as the same set of vignettes was read by all participants, generating one dependent variable for breach or no-breach. This uncovers the judgements made by participants (participant level) and affords comparisons across responses (vignette level).

As with most institutions, the large suburban Australian university used in this study has a list of ICT policy guidelines on the acceptable use of ICT resources and services. During enrolment, students agree to abide by the ICT policy and to use ICT resources and services for authorised purposes only. We conducted a study with student participants (Section 3.1) to understand how well they comprehend and abide by their university's ICT Code of Conduct.

We conducted (coronavirus compatible) online learning that primed two of the three groups with different content (G1: ICT policy group; G2: ethical principle group and G3: control group) as described in the experimental design and procedure in Section 3.2. Materials including the scenario and training design are included in Section 3.3. We received ethics approval for our study.

3.1 Recruitment

The focus of this study is on university students' understanding and application of the university's ICT Code of Conduct. We thus sought to recruit students using an available recruitment portal which provided access to students studying first-year psychology units who could choose our study from a list of approved studies to receive half an hour course credit. The majority of students in the available units are psychology students, but students from other departments might also enrol in these units and thus choose to participate in our study. As humanities and social sciences students, the participants recruited through this pool will be students who need ICT for their work, but who have not received formal training about cybersecurity at university. Thus, this convenience sample provided suitable participants for our study as research identifies that individuals without an ICT background (such as our cohort) are those most in need of such training. Further, as presented in the results, despite average scores for general knowledge of computers and of ethics, the cohort had low scores for knowledge of IT, cybersecurity, ethics in IT and ICT policy.

3.2 Experimental design and procedure

We examined whether students could identify the ethical issues (measuring their moral sensitivity) and could judge what to do (measuring their moral judgement) in a range of scenarios. We used the five AI4People ethical principles applied to cybersecurity (beneficence, non-maleficence, autonomy, justice and explicability) (Formosa *et al.*, 2021) to identify ICT misuses from the university's ICT policy "misuse schedule" (https://policies.XX.edu.au/download.php?id=371&version=1&associated) to design five scenario pairs. Each pair provides an example of a breach and a non-breach use of an ICT resource connected to the ethical principle. Each scenario had responses stating whether using ICT services and resources for this purpose is something the respondent agreed or disagreed with. The scenarios involved ethical dilemmas, which add complexity to the decision-making process and the consequences of taking a certain action. This allowed us to answer *RQ1: How can students' sensitivity to the ethical principles underlying their behaviour towards usage of ICT resources be measured?*

To test whether priming, and what kind, might influence participants' ethical responses, we conducted a between-subjects experiment with two factors (priming type: ICT policy or ethics principles) resulting in two experimental groups (group 1 and group 2) and one control group (group 3) which received no priming. Group 1 only received information about the university's ICT policy, relevant to the five scenario pairs, followed by a short quiz; Group 2 only received information about the five cybersecurity ethical principles (Formosa *et al.*, 2021) followed by a short quiz; and Group 3 received no information. Participants were randomly and evenly allocated to one of the three groups using Qualtrics Survey Software (QSS). This allowed us to answer *RQ2: Does priming students about (1) an ICT Code of Conduct or (2) relevant ethical principles influence their judgements about ICT policy compliance?*

Our experimental design is summarised in Figure 1. As controls, and to better understand our cohort, we captured potentially relevant data about participants. Participant familiarity and use of specific University ICT resources were measured on a 5-point Likert scale from "never" to "everyday". Knowledge of relevant topics (see Figure 1) was captured on a 5-point

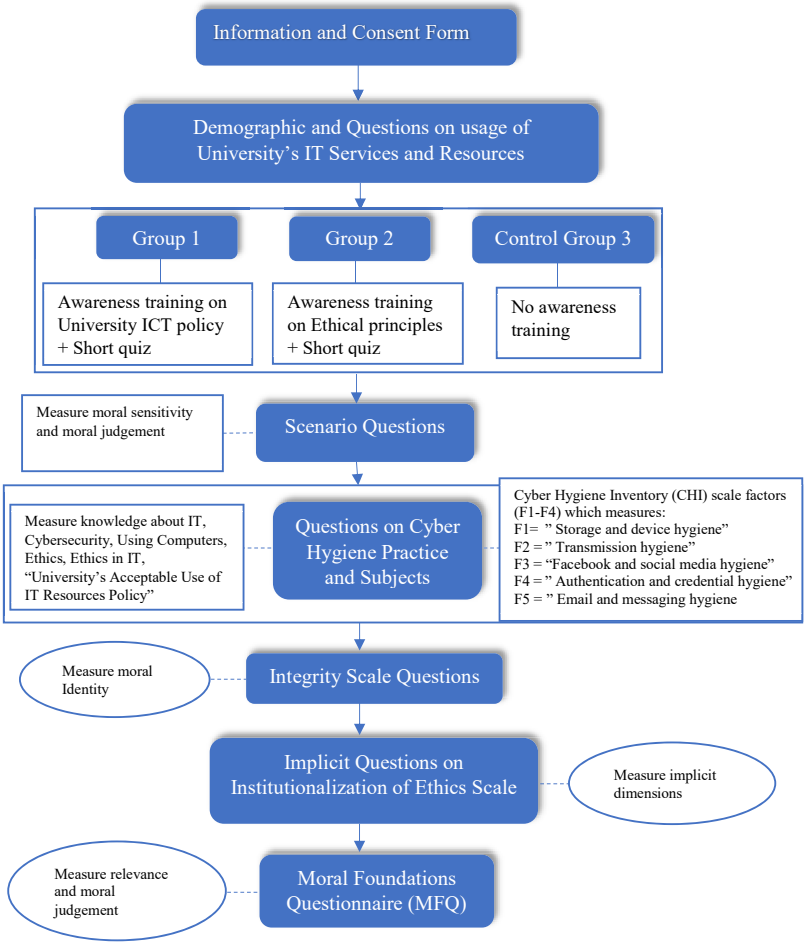


Figure 1.
Experimental design model

Likert scale from "terrible" to "excellent". Other scale details are in the referenced publications. To measure knowledge of cyber hygiene, we used the 18-item cyber hygiene inventory (CHI) (Vishwanath *et al.* (2020). To measure moral identity and commitment to principled ethical behaviour, we used the 18-item Integrity scale (Schlenker, 2008).

Singhapakdi and Vitell (2007) institutionalisation ethics scale measured students' commitment toward their university, as this could impact their ethical choices. However, we used only three constructs and 12-items from the internal scale viz. "importance of ethics, esprit de corps (team-spirit), and organizational commitment" (Singhapakdi and Vitell, 2007, p. 284), but not the fourth construct "job satisfaction" and the external scale, as these were irrelevant for student participants. Finally, we used the Moral Foundations Questionnaire (https://moralfoundations.org/questionnaires/) to measure participants' different moral foundations underlying their moral judgements.

We used IBM® SPSS® statistics version 25 (IBM Corp. Released, 2020 IBM SPSS Statistics for Windows) for statistical analyses and Microsoft Excel for data pre-processing. We conducted Kolmogorov and Shapiro–Wilk normality tests to determine the normal

distribution of data on scales. *T*-tests were used when comparing two groups, and ANOVA was used, plus post-hoc tests for significant results, when there were more than two groups. The significance level was set at 0.05. Thus, we performed one-way ANOVA to identify any significant differences between the three treatment groups in response to the scale items and independent *t*-tests across the cohort to identify significant gender (male/female) differences (as the latter has been identified in other work, e.g. Neigel *et al.*, 2020). To analyse responses to scenarios, we compared mean scores and standard deviations across groups for breach vs non-breach scenario responses and used a one-sample *t*-test to compare the overall breach versus non-breach scores. Thematic analysis was used to analyse the qualitative responses to the scenarios (Braun and Clarke, 2006).

3.3 Materials

Materials created for our experiment included the scenarios and two sets of priming materials, one on the university's ICT policy for group 1 and another on the five ethical principles identified above for group 2. These materials are provided in Appendix. A team of four individuals (three academics with combined expertise in cybersecurity, ethics and organisational behaviour, and one higher degree research candidate) iteratively created and reviewed the scenarios. The first version of the scenario is an ICT policy breach case and the second version is a non-breach case. A breach refers to a violation of the ICT policy. Figure 2 shows the pair for scenario 3 and the ethical principles embodied in the scenario. Section 4 presents results for all scenario pairs.

The scenarios are designed by mapping the university's "misuse" of ICT policy to our five ethical principles. For example, scenario 3.1 and 3.2 mapped the "misuse" of ICT policy that states ICT resources should not be used in ways that constitute "(x) breaching the University's Privacy Policy" to the underlying ethical principles of beneficence and non-maleficence (major) and justice and autonomy (minor). Due to the complexity, most scenarios had more than one ethical principle that could be mapped on to that ICT policy breach. The breach and non-breach scenarios also involve ethical dilemmas, where a breach scenario might involve unauthorised use of ICT resources and services for personal benefit or to cause harm to others, and non-breach scenarios might involve acceptable usage of ICT resources and services.

The 10 scenarios were presented in a fixed order to ensure that breach and no-breach cases alternated, and that breach and no-breach pairs were spaced at a maximum distance apart for participants. After reading each scenario, students selected their level of agreement with the question "*Is using University IT services and resources for this purpose something you agree or disagree with?*" on a seven-point scale from strongly agree to strongly disagree. Participants could then explain their answers in a free text response. To avoid fatigue, we limited the

Scenario 3.1: A friend starts a new private company and is looking to hire students who will soon be graduating. They ask you to share with them an email list of all your fellow classmates so that they can publicise these job opportunities. In order to help them, you locate a mailing list on a University server and forward it to your friend. The list you forward to your friend contains the first names, last names and personal email addresses of all your fellow classmates. Using the data from the mailing list, your friend uses their company's network to start sending bulk personalised emails to all your fellow classmates advertising the job opportunities.

Scenario 3.2: A friend starts a new private company and is looking to hire students who will soon be graduating. They ask you to share with them an email list of all your fellow classmates so that they can publicize these job opportunities. In order to help your friend, you send the details of the employment opportunities to your fellow classmates so that they can send their contact details to the company if they are interested in applying. Using the data, they received from the students who directly contacted them, your friend uses their company's network to start sending bulk personalized emails to those students who contacted them advertising the job opportunities.

[Relevant ethical principles: beneficence, non-maleficence, justice, autonomy]

Figure 2.
Scenario-pairs – mapping university's IT policy with cybersecurity ethical principles

number of scenarios per participant to ten (or five pairs) that took approximately 10 min in total out of the 30 min study to complete.

Participants from group 1 were primed by being first shown the parts of the policy which were relevant to the above five scenario pairs. They were then asked to complete a short three-question multiple-choice quiz to ensure policy understanding. Participants from group 2 were primed by being introduced to and given cybersecurity-specific definitions for the five ethical principles from the AI4People framework as applied to the cybersecurity context (see Formosa *et al.*, 2021). Participants then completed a short three-question multiple-choice quiz to ensure understanding of the five principles.

4. Results

4.1 Participant demographics

We first present demographic data to describe our sample. In total, 260 valid responses were received (excluding 13 records with incomplete data, resulting in imbalance in numbers across groups). Demographics of the group 1, group 2 and group 3 participants are shown in Table 1.

Participants were aged 17 [1]–56 years old, and the distribution of age groups across the groups was similar (average mean 21.5, average SD 6.56). In Australia, students over the age of 21 are considered mature age students (OpenUniversitiesAustralia), and students of any age can enrol for studying at the university. We have not discarded any data because all students were in the same first-year classes, and this represents the distribution that is likely to be found in Australian universities (studyanywhere). In terms of cultural groups, 52.01% of respondents were from Oceania (including Australia), with South-East Asia (15.02%), North African and Middle Eastern (8.79%) and Northwestern Europe (5.49%) being the next most common. All the participants were enrolled in a first-year psychology unit and gained entry to psychology program and thus have achieved good and similar educational outcomes previously. Hence, we did not examine their pre-university education as it was not relevant. Participant familiarity and use of specific university ICT resources are summarised in Table 2.

4.2 Results: group differences on outcome variables

Table 3 shows that all scales, except cyber hygiene, followed the normal distribution. Except for the Integrity scale, all scales showed high reliability ($\alpha > 0.75$). The Integrity scales' reliability increased (from $\alpha = 0.66$ to $\alpha = 0.7$) by deleting non-correlated items.

One-way ANOVA tests found no significant differences between the groups for the Moral Foundations Questionnaire, Integrity Scale or students' knowledge of relevant topics (see Table 4).

			Age		Main area of study**					
Group	*M*	*F*	μ	SD	PSY	BS	At	COMP	Other*	Total
ICT policy (G1)	30 (37%)	51 (63%)	21.51	5.86	63	3	1	1	13	81
Ethical principle (G2)	39 (42%)	53 (58%)	21.28	6.39	67	7	1	1	16	92
Control (G3)	35 (40%)	52 (60%)	21.94	7.36	65	7	3	0	12	87
Total	104 (40%)	156 (60%)	Avg = 21.5	Avg = 6.56	195	17	5	2	41	260

Note(s): *M* = male, *F* = female. * Human Science, Health, Science, Speech and Hearing, Law, Sociology, Criminology, Education, Allied Health, Clinical Science, Medical, Anatomy, Linguistics. **PSY=Psychology, BS=Business, AT = Arts, COMP=Computer

Table 1. Demographics across groups

For the Cyber Hygiene Scale, we found no significant differences between the three groups, but we did find a significant difference for the storage and device hygiene construct of the cyber hygiene scale for $p = 0.001$ when compared by gender. Here males (mean = 11.10, SD = 4.29) score was higher than females (mean = 9.08, SD = 3.92) indicating their awareness of storage and device hygiene practices. Males exhibited better cyber hygiene practices than females (Cain *et al.*, 2018). Males showed good cyberhygiene practices such as virus scan on new USB, downloading licensed software, creating strong passwords, checking the authentication while doing online transactions, installing firewalls and setting up two-factor authentication (Vishwanath *et al.*, 2020; Cain *et al.*, 2018). Females showed good cyberhygiene practice for managing their social media account and checking for emails from unknown senders (Vishwanath *et al.*, 2020). It is also observed that women showed higher consciousness towards improper use of computer technology (such as data encryption,

Table 2.
Usage of IT services and resources of the university

IT services and resources	Percentage
iLearn LMS	65.57% (everyday), 27.47% (often)
Wi-Fi	6.23% (everyday), 27.11% (often)
Virtual private network (VPN)	72.89% (never), 17.22% (rarely)
Website	6.96% (everyday), 26.74% (often)
IT Helpdesk	41.03% (never), 37.00% (rarely)
Library	4.40% (everyday), 39.93% (often)
Email	30.77% (everyday), 40.66% (often)
Licensed software*	15.75% (everyday), 28.21% (often)
Computer labs	64.47% (never), 23.44% (rarely)

Note(s): * Office 365, Endnote, etc

Table 3.
Normality test for the scales

Profiling measures	Kolmogorov–Smirnova Statistic	Df	*p*-value	Shapiro–Wilk Statistic	Df	*p*-value
Cyber hygiene Scale	0.042	260	0.200*	0.984	260	0.006
Integrity Scale	0.063	260	0.015	0.993	260	0.233
Institutionalisation of Ethics Scale	0.065	260	0.011	0.990	260	0.080
Moral Foundation Questionnaire Part 1	0.053	260	0.079	0.992	260	0.163
Moral Foundation Questionnaire Part 2	0.051	260	0.200*	0.994	260	0.394

Note(s): * This is a lower bound of the true significance. a. Lilliefors Significance Correction

Table 4.
Comparison of means for knowledge about subjects across groups

Knowledge on subjects	ICT policy group(G1) *M*	SD	Ethical principle group(G2) *M*	SD	Control group(G3) *μ*	SD	One-way ANOVA *f*-value	*p*-value
Knowledge of IT (1–5)i	2.62	0.94	2.76	0.89	2.72	0.91	0.562	0.571
Knowledge of computers (1–5)i	3.51	0.85	3.47	0.88	3.64	0.77	1.073	0.344
Knowledge of cybersecurity (1–5)i	2.70	1.0	2.65	0.91	2.66	0.86	0.080	0.923
Knowledge of ethics (1–5)i	3.59	0.94	3.70	0.78	3.72	0.91	0.517	0.597
Knowledge of ethics in IT (1–5)i	2.80	0.88	2.62	0.82	2.80	0.92	1.305	0.273
Knowledge of university's IT policy (1–5)i	2.77	0.93	2.76	0.96	2.72	0.91	0.050	0.951

Note(s): [i] min and maximum range of possible values

inserting a virus, banned games) (Gattiker and Kelley, 1999). These human factors can be used to predict males' and females' attitude and knowledge towards cyberhygiene behaviour (Neigel *et al.*, 2020).

For the Institutionalisation of Ethics scale, we found no significant gender differences, but we did find a significant difference between the three groups for the organisational commitment (OC) construct, $p = 0.047$. This shows the positive relationship between students' ethical values and their commitment towards the university (Singhapakdi and Vitell, 2007). People with organisational commitment have compliant behaviour towards the information security policy (ISP) and exhibit positive influence to their subordinates (Liu *et al.*, 2020). However, individuals who are more committed towards the organisation have higher levels of responsibility to protect the organisation from threats (Posey *et al.*, 2015). The response given by high organisationally committed individuals are used to mitigate the threats that may affect the organisation from the individual with less organisational commitment (Posey *et al.*, 2015). As we found the significant result for organisational commitment, we conducted post-hoc Tukey HSD test and found that group 1 and group 3 had p-value = 0.052, which is close to $p < 0.05$. Hence, we conducted a Bonferroni adjustment post-hoc test for the third construct of the scale and found that group 1 and group 3 had p-value = 0.059, which showed that the two groups were not significantly different. Therefore, we conducted a Dunnett-t (2-sided) post-hoc analysis test for the same construct which compares the experimental groups (G1 and G2) with the control group (G3) and observed a significant difference between group 1 and group 3 (p-value = 0.037). However, there was no significant difference between group 2 and group 3 (p-value = 0.11).

4.3 Results: group differences based on scenario responses

The one-sample t-test results showed significant differences between participants' responses for all breach vs non-breach scenario pairs ($p < 0.001$). Independent sample t-tests to compare scenario responses based on gender found no significant differences. A comparison of mean scores and standard deviations across groups for breach vs non-breach scenario responses is shown in Table 5. The lowest mean scores for the breach versions were 3.11 (G1), 2.91 (G3), 2.00 (G3), 1.704 (G3), and 2.75 (G3), indicated in orange colour in Table 5. Based on a 7-point Likert scale, all groups disagreed with the behaviour in breach scenarios. However, the

Scenario-pair	Version	ICT policy group(G1)		Ethical principle group(G2)		Control group(G3)		One-way ANOVA	
		μ	SD	M	SD	μ	SD	f-value	p-value
1. Hosting a website	1.1	3.11	1.50	3.47	1.82	3.37	1.84	0.95	0.38
	1.2	5.19	1.71	5.38	1.82	5.38	2.04	0.30	0.73
2. Downloading series to watch	2.1	3.21	1.77	3.43	1.78	2.91	1.76	1.98	0.13
	2.2	3.93	1.64	4.49	1.55	4.06	1.92	2.61	0.07
3. Sharing email list of fellow classmates to others	3.1	2.41	1.53	2.42	1.54	2.00	1.17	2.47	0.08
	3.2	4.41	2.04	4.82	1.93	4.38	2.20	1.25	0.28
4. Inserting unattended USB into university computer	4.1	2.30	1.55	1.88	1.16	1.70	1.05	4.41	0.01*
	4.2	3.85	1.80	3.77	1.95	3.23	1.82	2.84	0.06
5. Third party software download	5.1	3.21	1.67	2.83	1.69	2.75	1.96	1.59	0.20
	5.2	5.07	2.10	5.41	1.98	5.43	1.85	0.846	0.43

Note(s): *There is a significant difference at $p < 0.05$. Bluecolour = highest non-breach, orangecolour = lowest score breach

Table 5.
One-way ANOVA comparing breach vs non-breach group means

control group's mean scores for breach scenarios were lower than the experimental groups for all scenarios except scenario 1.

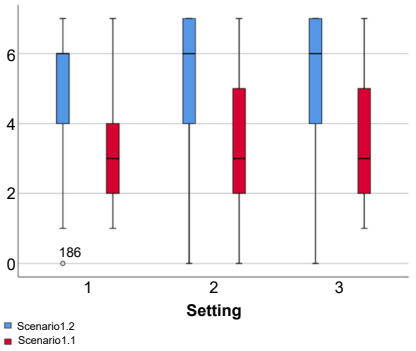
There was only a statistically significant difference for breach scenario 4.1 between the three groups which shows that participants considered inserting the unattended USB as a maleficent act and this shows their right judgement (Gattiker and Kelley, 1999). The maximum mean score for the breach versions were 3.47, 3.43, 2.42, 2.30, and 3.21 (all below 4 and an average of 2.96 < 3 which indicates disagreement with breaching behaviour) which showed all three groups were able to identify the breach in the scenarios. The highest mean scores (indicated in blue colour in Table 5) for non-breach versions are 5.38 (G2, G3), 4.49 (G2), 4.82 (G2), 3.85 (G1), and 5.43 (G3).

There was no significant difference for non-breach versions between the groups. The lowest mean score for the non-breach versions of the scenarios were 5.19, 3.93, 4.38, 3.23 and 5.07 (average > 4) which showed the three groups were able to identify the ethical dilemma for non-breach scenarios 1.2 and 5.2 which were about hosting a website as part of their assignment from their lecturer and downloading licensed software. However, the three groups failed to identify ethical dilemma for other non-breach scenarios 2.2, 3.2 and 4.2 which were about downloading series of episodes in low resolution using university Wi-Fi, sharing fellow classmates email addresses with their acknowledgement and inserting unattended USB to learn about virus mitigation. Figure 3 (a-e) represents the box-plot comparisons of scenario-pair (breach vs non-breach, 1.1 to 5.1 vs 1.2 to 1.5, respectively) versions for the three groups G1, G2, and G3 (called setting 1, 2 and 3, respectively). We can see that the mean score is higher for all the non-breach cases than the breach cases for all scenarios. In scenario 2, the mean breach and non-breach scores were close, particularly for G1, and there was more overlap between the breach and non-breach scores. Looking at this scenario, the student had to make a judgement call about how much download use is reasonable.

We did post-hoc tests to examine whether groups had significant differences across each scenario. We only found a significant difference between the ICT policy group and the control group for scenario 4.1 ($p = 0.012$, $p < 0.05$). Due to the wide age span, we conducted sample *t*-test of the responses to the 10 scenarios between age groups 17–20 (187 participants) and 21+ (73 participants); and 17–34 (239 participants) and 35+ ((21 participants). The results comparing age groups 17–20 and 21+ showed significant difference for scenarios 1.1, 1.2, 2.2, and 3.1 (see Appendix 2 Table A1). The results comparing age groups 17–34 and 34+ (see Appendix 2 Table A2) showed significant differences for scenarios 1.1, 1.2, 2.2, 5.1 and 5.2. These are discussed later.

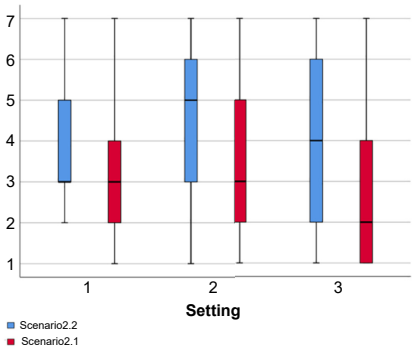
4.4 Results: qualitative data

At the end of every scenario, participants were asked to explain the reasoning for their choices. We received 240 useable responses for each scenario. Although the statistical analyses did not reveal significant differences following priming, participants' comments tended to use language from the priming as part of their reflections. This indicated the priming had some impact. For example, the ICT policy group used terms from their priming information, such as "misuse of IT, breach of privacy/confidentiality, and, infringement of privacy without their consent"; the ethical principle group used terms from their priming information, such as "invasion of privacy, consent, beneficial, autonomy, harmful, not right, not fair, and justice"; and the control group (who received no information) used terms such as "illegal acts, breach of academic policy". Two participants (1 – male, 1 – female) expressed unawareness of IT policy and commented "I do not know the university wi-fi policy", "I do not know what the university's guidelines (are) on using their Wi-Fi", and "I do not know enough about the risks of computer viruses". In some cases, participants were unable to make judgements, expressed in phrases such as "there is a bit of confusion", "I am bit on the agree/disagree side for this scenario" or just wrote "agree" or "not sure". Table 6 outlines the themes



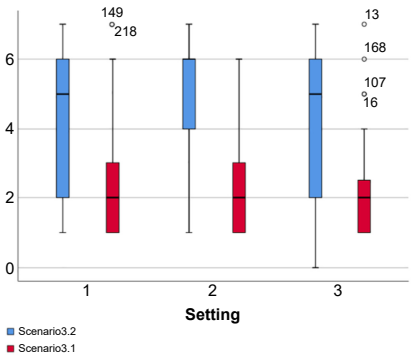
Scenario 1.1 vs. Scenario 1.2

(a)



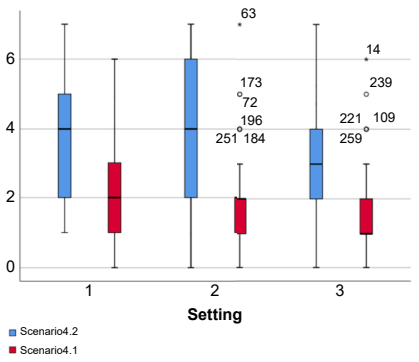
Scenario 2.1 vs. Scenario 2.2

(b)



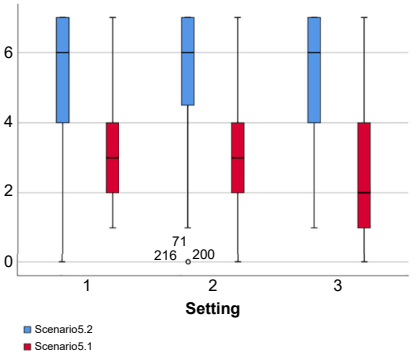
Scenario 3.1 vs. Scenario 3.2

(c)



Scenario 4.1 vs. Scenario 4.2

(d)



Scenario 5.1 vs. Scenario 5.2

(e)

Figure 3.
(a–e): Graphs comparing breach and non-breach versions of scenario-pairs using box-plot

Themes/Principles	ICT policy group 1	Ethical principle group 2	Control group 3
Unethical/ misconduct *Non-Maleficence; Justice*	19 comments. Example: "the software is pirated and therefore unethical/ could be constituted as a misconduct"	15 comments. Example: "it was unethical to use someone's equipment and possibly damage university services and recourses"	27 comments. Example: "using university Wi-Fi for personal use and is unethical"
Breach of consent *Autonomy*	33 comments. Example: "exploitation of obtaining the private information of other students without their consent"	50 comments. Example: "sharing private info without consent is not right"	50 comments. Example: "someone else's USB should not be used without their consent"
Invasion of privacy *Non-Maleficence; autonomy*	30 comments. Example: "breached someone's privacy of looking at their USB"	26 comments. Example: "This is a major breach of privacy and those emails may be highly unwanted by many students"	24 comments. Example: "It is an invasion of privacy as none of the classmates have given their permission"
Non-beneficial, causing harm, and potential risk **Non-***Maleficence Beneficence*	4 comments. Example: "beneficial in study and not causing harm"	12 comments. Example: "university IT services is there to help support students for educational purposes and it should not often be utilised to benefit"	8 comments. Example: "could harm future students using the same computers"
Piracy is illegal *Justice*	17 comments. Example: "pirated software sounds illegal"	23 comments. Example: "Should not use pirated software, this is illegal"	22 comments. Example: "Pirating stuff is illegal and 3rd party software can be malicious"
Against the norms of university and IT-policy *Justice beneficence*	7 comments. Example: "commercial benefit is against the IT policy"	7 comments. Example: "personal use of wifi connection in their codes of conduct then i dont see the problem"	11 comments. Example: "using pirated software for assessments should is breach of academic policy"
Dishonesty and theft *Justice; beneficence*	0 comments*	0 comments*	8 comments. Example: "dishonesty and unethical because student not should builds and tests the website on University servers for their own personal benefit"
Infringing/copyright laws *Justice*	7 comments. Example: "They cannot use the university software because of the copyright belong to university"	1 comment. Example: "as it is pirate content, the university may be liable for penalties as they are breaking the copyright law"	0 comments*
Authorised use only *Autonomy*	4 comments. Example: "University IT services are for authorised use only"	2 comments. Example: "authorised the third party downloads, is ok"	0 comments*

Table 6.
Frequency and sample quotes from participants' comments showing higher-level themes between the three groups

Note(s): Numbers represent the number of times this theme was mentioned in the comments given by students *The themes with 0 comments are listed because the theme was not mentioned by participants in the given group/s

generated by each group and the total number of participants who used these themes in their comments. The uncovered themes were mapped to the relevant ethical principle. The frequency is determined by the number of occurrences of that particular theme in the comments given by the participants.

The majority (more than 90%) of responses affirmed that using the university's IT resources and services unethically was something they disagreed with. Examples of common responses from people who disagreed with the non-breach scenarios include "The software, as provided by the University, is for the purpose of study and assessment, not for commercial usage" (Scenario 1.2: Hosting a website); "It is a little excessive to download 10 episodes and that too on high resolution" (Scenario 2.2: Downloading series to watch); "it's a breach of privacy because students have not given their consent" (Scenario 3.2: Sharing email list of fellow classmates to others); "This could potentially harm the University servers as unknown information could appear on this USB drive" and users should "inform the IT department" (Scenario 4.2: Inserting unattended USB into university computer); "Pirated software is illegal" (Scenario 5.2: Third party software download).

However, some participants agreed with the behaviour described in the breach case scenarios. Examples of these comments include: "people pay a lot of money to [go to] university, they have a right to use the Internet regardless of their personal use", and "it is beneficial to a student to use (the) server to host website of their employer" (Scenario 1.1: Hosting a website); "as long as the student is not breaking any laws or rules and students can use the WIFI as they please whilst they are at university as they pay fees" (Scenario 2.1: Downloading series to watch); "Agree because you are helping them by giving them jobs opportunity and it's helpful finding career pathways through sharing" (Scenario 3.1: Sharing email list of fellow classmates to others); "I think it's okay to use USB's but if it's causing viruses then that's a problem and it is for educational purpose" (Scenario 4.1: Inserting unattended USB into university computer); "downloading pirated software using university network is Ok and students pay for it and used for educational purposes/assignment purpose" (Scenario 5.1: Third party software download).

The themes were used to show that the participants reflected on the key terms from the ICT policy or ethical principles. Themes were identified for all groups. Themes with 0 comments indicate that the theme was not mentioned by the members of that particular group, although members of other groups do mention the theme (which is why we include it). For example, the theme around infringing copyright was mentioned by both members of the ICT policy group 1 and the ethical principle group 2, but were not mentioned by control group 3 (hence the 0 comments for that respective group was indicated with respect to the theme).

Despite the fixed ordering of scenarios to ensure breach and non-breach scenario pairs were separated, some participants connected the two and identified the differences between the two versions of the scenarios. For example, one participant noted that "The key difference in comparison to the first Netflix scenario, is that the student is now using higher quality streaming (that) may impact the speed of the Internet" (Scenario 2.1 vs 2.2), which clearly shows the participant was reflecting on the differences between the breach and non-breach versions. Lastly, 44 participants were "unsure" about their decisions, and nine said, "I do not understand or know".

5. Discussion

Results showed significant differences between the breach and non-breach responses for all scenarios. Positively, across groups students showed significantly greater agreement with non-breach scenarios than breach scenarios, suggesting they could discern appropriate from inappropriate ICT resources usage. However, the inclusion of priming (on ICT policy or the five ethical principles) did not yield a significant difference overall. For the one observed

significant difference in responses between the control and ICT policy group, it was counterintuitively the control group who were better able to identify the breach. We now return to our two research questions.

To answer *RQ1 (How can students' sensitivity to the ethical principles underlying their behaviour towards usage of ICT resources be measured?)*, we captured students' responses to five scenario pairs containing ethical dilemmas relating to breach and non-breach usage of the university's IT resources. Each scenario pair was based on one of the university's specified "misuses" of IT resources and then mapped to the five ethical principles as summarised in Table 7.

Scenario pairs 1 and 2 sensitised participants to the ethical principles of non-maleficence (e.g. harming other students or the university) and justice (e.g. unfair advantages). Scenario pair 3 sensitised participants to the principles of beneficence (e.g. possible employment benefits from sharing), non-maleficence (e.g. students receiving unsolicited emails), justice (e.g. privacy right violations) and autonomy (e.g. no consent to share). The fourth scenario-pair sensitised participants to the ethical principles of beneficence (e.g. benefits from using the drive), non-maleficence (e.g. it could infect the university's computers), explicability (e.g. their actions lack accountability) and justice (e.g. violate the university's property rights). The fifth scenario-pair sensitised participants to the ethical principles of justice (e.g. software owner's rights), autonomy (e.g. lack of consent) and non-maleficence (e.g. financial harms to software developer). Differences in responses to scenarios can be due to influence of human factors such as personal ethical beliefs and intentions to adopt ICT policies (Johnson, 2018; Schlenker, 2008). Some responses also indicate the influence of prosocial altruistic behaviour which might have led to participants' decision not to use university's ICT resources for personal usage, not to disclose their fellow classmates details to others and being thoughtful to others by returning the unattended/lost USB (Bar-Tal, 1976; Rosenhan, 1972).

Our results showed that these scenarios provided a means to connect an ICT Code of Conduct with ethical principles and to measure students' ethical responses to appropriate and inappropriate usage of ICT resources. Validating our scenario design, participants' breach scores were significantly less than the non-breach scores for all scenario pairs. The average scores for all breach scenarios showed disagreement (below 4 on a 7-point scale) with the described usage, while average scores for four of the five non-breach scenarios showed agreement (above 4 on a 7 point-scale). These results show that on average students were able to identify the ethical dilemma in the breach scenarios and students could recognise appropriate uses of ICT resources in the non-breach scenarios. Scenario 4, concerning using an unidentified USB, is an exception and is discussed further below. The scenario instrument was able to measure students' knowledge of appropriate ethical usage of ICT resources and services. Universities can use this instrument (adapted to their ICT Policy) to create

Table 7.
ICT policy scenarios for measuring students' ethical sensitivity towards usage of ICT resources

Scenarios/Principles	NM	JUS	BEN	AUT	EXP
Using IT for hosting a website for unauthorised/authorised purposes	X	X			
Impose an unreasonable burden or not on IT resources by downloading a series on Netflix	X	X			
Breach or not breach the privacy policy by sharing fellow classmates' email addresses	X	X	X	X	
To take care and maintain IT resources by not inserting an unattended USB flash drive	X	X	X		X
Infringement of intellectual property rights by downloading pirated software or licenced software	X	X		X	

Note(s): Non-Maleficence – NM, Justice – JUS, Beneficence – BEN, Autonomy – AUT, Explicability – EXP

awareness training for ethical ICT usage among students without an ICT background, as they are the most vulnerable group for cyber-attacks and identified as the weakest link in the organisation regarding appropriate cybersecurity behaviours (Jamil and Shah, 2014; Yan *et al.*, 2018).

For RQ2 (*Does priming students about (1) an ICT Code of Conduct or (2) relevant ethical principles influence their judgements about ICT policy compliance?*), we compared the responses to the scenarios for the ICT policy priming, ethical principle priming, and control groups. There was a nearly equal distribution of gender, age, and area of study of the participants across the three groups. There were significant differences for only one organisational commitment construct (institutionalisation of ethics scale); however, there were no significant differences for any of the other scale instrument's constructs. Looking at the scores overall, we can see that the three groups were similar in their responses, giving low scores for breach and high scores for non-breach. There was one significant difference in responses for scenario 4.1 "inserting an attended USB into university computer" between the ICT policy and control group. Perhaps the control group applied their common sense to respond to the question about appropriate resource usage, whereas some participants in the ICT Policy group, and to a lesser extent the ethical principles group, failed to see the connection with the use of IT resources as the priming materials did not explicitly mention USB usage. Overall, it appears that most students are aware of the potential dangers of such a practice as we note that on average all three groups did not agree with the breach in this scenario (their scores were less than 3 on 7-point Likert scale). Although we do not know if their disagreement would match their actual behaviour in practice, this is a positive finding, as the study by Tischer *et al.* (2016) who placed 297 USB drives containing malware around a university campus found that for altruistic reasons, i.e. trying to find the owner, most students did insert the unattended USB drive. The decision to assist the owner of the USB (by choosing beneficence to others over potential harm) could be evidence of prosocial behaviour. According to the theory of prosocial behaviour, individuals exhibit altruism when they act to benefit others at their own cost (Rosenhan, 1972).

There was no other statistically significant difference between the experimental group who received the priming on the ICT policy or the five ethical principles and the control group. We note, however, that the priming interventions did seem to raise some awareness of either the ICT Policy or ethical principles because individuals in these groups used terms specific to the priming they received in their qualitative reflections. This suggests that they did learn something from being primed, but what they learned did not produce a significant change in their behaviour. This could have been because most participants could already identify the difference between breach and non-breach cases as demonstrated by all groups, including the control group who received no priming, on average agreed with the behaviour in non-breach scenarios and disagreed with the behaviour in breach scenarios. Priming may have given participants the language to better describe their behaviours.

Analysis of scenario responses by age (see Appendix 2), regardless of group, revealed some interesting, though not surprising results. The older age group were more cautious than the younger age groups which indicates their greater intention not to misuse university resources. The possibilities for such behaviour can be their previous work experience, prosocial behaviour and intention to help others (Lindenberg, 2006; Rosenhan, 1972). The older participants viewed moral domain scenarios (e.g. downloading pirated software) as acts of maleficence and personal domain scenarios (e.g. sharing fellow-classmates emails with their consent, hosting a website for learning) as acts of beneficence (Gattiker and Kelley, 1999). Our analyses show that younger students were less aware of proper organisational IT usage. We thus further conclude that the maturity, identified through age, of the student is likely to influence their ability to recognise inappropriate cyberhygiene behaviours. However, we note that, on average, both recent school leavers and mature age students were able to

recognise breaches and acceptable behaviours. It could be assumed that older students have work experience that has exposed them to appropriate IT usage behaviours in other organisations. It also suggests a greater need for training of recent school leavers (under 21 years of age) in appropriate ICT usage. This will also be important to facilitate "work readiness" so that students are aware of ICT Codes of Conduct/Policy and follow them with their employer; which is supported by other literature where they conducted a vignettes-based study to assess individuals' ethical use of computer technology and their results found that older users have a higher moral stance than younger users (Gattiker and Kelley, 1999). However, their study was not student focused.

Our study contributes to the emerging, but competing, evidence on the effectiveness of priming in a cybersecurity context, and lends weight to studies that show it is not necessarily effective for activating system 2 thinking discussed earlier either for students (as found by Mazar *et al.* (2008)) or in a cybersecurity context (as found by Junger *et al.* (2017)). For example, a similar study by McNamara *et al.* (2018) gave explicit instructions on the ACM code of ethics to software engineering professionals and students to understand the influence of the code on participants' ethical decision-making. That study also showed no significant difference between the control group and the experimental group that viewed the code of ethics. Even though our priming interventions were longer than those used by McNamara *et al.* (2018) and we included a control group, we still could not quantitatively demonstrate that the intervention significantly affected users' knowledge or planned behaviours. Overall, our findings suggest that small interventions, such as those undertaken in this study, are likely to have small, if any, impacts on behaviour.

What our work does suggest though is that more nuanced and targeted approaches to priming may be needed. The need for specificity is somewhat supported by the superior ability of the control group to identify the breach in the USB-related scenario; suggesting that priming that is too general and may have a confounding effect when scenarios are highly specific. Selecting the right type or combining more than one type of priming may be needed. For example, priming can take many forms, such as affective (i.e. the use of "affect-loaded stimuli" to influence emotions and feelings) and behavioural (i.e. a primer targeted to alter behaviour) priming (Minton *et al.*, 2017). The latter category constitutes procedural priming (i.e. priming to follow a certain procedure for a task) and goal priming (i.e. priming that leads to behaviours that are consistent with one's goals) (Minton *et al.*, 2017). Forms of procedural priming are more resilient over time than other forms, particularly where procedural knowledge is activated which prompts individuals to follow a designated process and exert greater cognitive effort, or system 2 thinking, to reach a particular end (Minton *et al.*, 2017). As Rosoff *et al.* (2013) found that negatively framed messages focused on risks and adverse consequences can prompt safer cyber behaviour, it may be that the use of affective priming will have more of an impact as it focuses on the negative implications for individuals of poor cyberhygiene behaviour. Given that Shieh and Rajivan (2021) show that some forms of priming have only short-lived, momentary effects on user behaviour, it is also likely that single-shot priming interventions alone are not sufficient in a cybersecurity context. More intensive interventions, potentially involving longer or multiple sessions for reinforcement, may be required to have a significant effect. Such longitudinal interventions would also help counter the fact that cyber threats are dynamic and can become more sophisticated over time (Richardson *et al.*, 2020). It may also be that since priming effects can degrade fairly quickly, they should be targeted at the point in time that a user may be faced with a cyberethical dilemma to activate system 2 thinking at the very time it is required. Finally, other awareness-raising methods could be used to complement priming, such as encouraging students to follow the ICT Code of Conduct by providing support from a "faculty handbook" that can explain policies and processes in addition to course information (Rezaee *et al.*, 2001, p. 178), although whether this makes a significant difference remains unclear.

6. Conclusion, limitations, and future work

We investigated whether priming on a university's ICT policy or cybersecurity relevant ethical principles changed students' attitudes and behavioural intentions (Johnson, 2018) and affected their cybersecurity ethical judgements. We found that groups that received priming concerning either the ICT policy or the ethical principles did not do any better compared to the control group.

The main limitations of our research are that all the participants were from the same university, our sample size was small, and a large proportion of the population was from one department. As psychology students may have received ethics and the ethical use of data training, it is possible that these students may not be representative of other cohorts who may be more or less aware of their institutional Code of Conduct for safe cyber hygiene practices. We recommend replicating the study with other populations from a wider range of disciplines, postgraduate and undergraduate students, and different institutions. Further, different ICT Code of Conduct implementations might have different approaches to training, awareness, and monitoring. Since the presented scenarios only cover certain aspects of the ICT policy of the university, different scenarios could cover other aspects of the policy. Further, our scenario questions measure the participants' intentions, which may not reflect their actual cybersecurity ethical decisions. Other factors, such as age and cultural group, could also be investigated further to determine whether these influence students' responses.

The priming material we provided was intentionally brief to minimise the cognitive effort required and to encourage students to read it in full. The quiz asked immediately after the priming information was provided aimed to further incentivise students to read and comprehend the material. However, participants could not access the priming materials while responding to the scenarios. Providing extended training and/or making the priming materials available while responding to the scenarios might have generated more impact. The priming materials and vignettes were designed to be suitable for non-technical cohorts (such as psychology students), and future informational material could also be suitably designed to address both technical and/or non-technical cohorts.

Our study did not find significant value in using priming to improve ethical judgements concerning compliance with ICT policy. Further research is needed to examine how much and what type of priming might have a significant impact. In particular, there is a need for more innovative approaches involving interactive learning methods, such as gamification (Hart *et al.*, 2020), for developing ethical reasoning among students when making cybersecurity judgements. This could help students to make ethical choices in their cybersecurity practices and promote good cyber hygiene. Priming provides a lens through which students can be sensitised to make ethical decisions. This study can also be extended to investigate educational interventions for other cyber ethical problems. Longer and more impactful interventions might be effective in guiding the target audience towards compliance with ICT policy (Hendrix *et al.*, 2016). Looking beyond universities and students, this scenario, policy and principle-based approach could be adapted to train and creating awareness among IT/cyber professional employees. Regardless of the organisation or target, there remains a lack of understanding of what type of education might be beneficial to eliminate unethical cyber hygiene behaviour (Cain *et al.*, 2018). Solutions that are developed need to be feasible and practicable for the context given the current lack of resources to develop, deliver or evaluate such interventions, meriting further exploration of priming-based approaches.

Note

1. The Ethics Committee has agreed that university students who are 17 years of age, but are studying at a university level, are equivalent to a participant who is 18 years of age. 17-year-old participants may enrol in studies that are targeted to 18+ years providing that the study does not state "***strictly***" 18 years, or that there is a specific reason for people under the age of 18 not to participate (e.g. the study relates to the consumption of alcohol).

References

Aguinis, H. and Bradley, K.J. (2014), "Best practice recommendations for designing and implementing experimental vignette methodology studies", *Organizational Research Methods*, Vol. 17 No. 4, pp. 351-371.

Alqahtani, H. and Kavakli-Thorne, M. (2020), "Does decision-making style predict individuals' cybersecurity avoidance behaviour?", *International Conference on Human-Computer Interaction*, pp. 32-50.

Ariely, D. (2012), "Why we lie", *Wall Street Journal*, May 26-27, 2012, pp. C1-C2.

Bar-Tal, D. (1976), *Prosocial Behavior: Theory and Research*, Hemisphere Publishing Corp, London.

Beauchamp, T.L. and Childress, J.F. (2001), *Principles of Biomedical Ethics*, Oxford University Press, New York, NY.

Bia, M. and Kalika, M. (2007), "Adopting an ICT code of conduct: an empirical study of organizational factors", *Journal of Enterprise Information Management*, Vol. 20 No. 4, pp. 432-446, doi: 10.1108/17410390710772704.

Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N.C., Campbell, R.H. and Bashir, M. (2018), "A case study-based cybersecurity ethics curriculum", *2018 (USENIX) Workshop on Advances in Security Education (ASE18)*.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101.

Cain, A.A., Edwards, M.E. and Still, J.D. (2018), "An exploratory study of cyber hygiene behaviors and knowledge", *Journal of Information Security and Applications*, Vol. 42, pp. 36-45.

Cram, W.A., Proudfoot, J. and D'Arcy, J. (2017), "Seeing the forest and the trees: a meta-analysis of information security policy compliance literature", *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Denisova-Schmidt, E. (2018), "Corruption, the lack of academic integrity and other ethical issues in higher education: what can be done within the Bologna process?", *European Higher Education Area: The Impact of Past and Future Policies*, Springer, Cham, pp. 61-75.

Dupuis, M.J. (2017), "Cyber security for everyone: an introductory course for non-technical majors", *Journal of Cybersecurity Education, Research and Practice*, Vol. 2017 No. 1, p. 3.

Floridi, L. and Cowls, J. (2019), "A united framework of five principles for AI in society", *Harvard Data Science Review*, Vol. 1 No. 1, pp. 1-15.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U. and Rossi, F. (2018), "AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations", *Minds and Machines*, Vol. 28 No. 4, pp. 689-707.

Formosa, P., Wilson, M. and Richards, D. (2021), "A principlist framework for cybersecurity ethics", *Computers and Security*, Vol. 109, p. 102382.

Garrison, C.P. and Posey, O.G. (2006), "Computer security awareness of accounting students", *Southwest Decision Sciences Thirty-Sixth Annual Meeting*.

Gattiker, U.E. and Kelley, H. (1999), "Morality and computers: attitudes and differences in moral judgments", *Information Systems Research*, Vol. 10 No. 3, pp. 233-254.

Han, W., Ada, S., Sharman, R. and Rao, H.R. (2015), "Campus emergency notification systems", *Mis Quarterly*, Vol. 39 No. 4, pp. 909-930.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020), "Riskio: a serious game for cyber security awareness and education", *Computers and Security*, Vol. 95, p. 101827.

Healy, M. and Iles, J. (2002), "The establishment and enforcement of codes", *Journal of Business Ethics*, Vol. 39 Nos 1-2, pp. 117-124.

Hendrix, M., Al-Sherbaz, A. and Bloom, V. (2016), "Game based cyber security training: are serious games suitable for cyber security training?", *International Journal of Serious Games*, Vol. 3 No. 1, pp. 53-61.

IBM Corp. Released (2020), *IBM SPSS Statistics for Windows, V.A.*, IBM Corporation, New York.

Jamal, A., Ferdoos, A., Zaman, M. and Hussain, M. (2016), "Cyber-ethics and the perceptions of Internet users: a case study of university students of Islamabad", *Pakistan Journal of Information Management and Libraries*, Vol. 16 December 1, 2015, pp. 8-20, doi: 10.47657/201516725.

Jamil, M. and Shah, J. (2014), "Perception of undergraduates about computer and Internet ethics in Pakistan", *Nigerian Journal of Technology*, Vol. 33 No. 4, pp. 512-522.

Johnson, E.L. (2018), "Factors influencing undergraduate students' intention to adopt information security policies: a correlational study", Capella University.

Junger, M., Montoya, L., Hartel, P. and Heydari, M. (2017), "Towards the normalization of cybercrime victimization: a routine activities analysis of cybercrime in Europe", *2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, pp. 1-8.

Kim, E.B. (2013), "Information security awareness status of business college: undergraduate students", *Information Security Journal: A Global Perspective*, Vol. 22 No. 4, pp. 171-179.

Kruger, R. (2003), "Discussing cyber ethics with students is critical", *The Social Studies*, Vol. 94 No. 4, pp. 188-189.

Kvaran, T., Nichols, S. and Sanfey, A. (2013), "The effect of analytic and experiential modes of thought on moral judgment", *Progress in Brain Research*, Vol. 202, pp. 187-196.

Leonard, L.N. and Cronan, T.P. (2005), "Attitude toward ethical behavior in computer use: a shifting model", *Industrial Management and Data Systems*, Vol. 105 No. 9, pp. 1150-1171, doi: 10.1108/02635570510633239.

Lindenberg, S. (2006), "Prosocial behavior, solidarity, and framing processes", in Fetchenhauer, D., Flache, A., Buunk, B. and Lindenberg, S. (Eds), *Solidarity and Prosocial Behavior. Critical Issues in Social Justice*, Springer, Boston, MA, doi: 10.1007/0-387-28032-4_2.

Liu, C., Wang, N. and Liang, H. (2020), "Motivating information security policy compliance: the critical role of supervisor-subordinate guanxi and organizational commitment", *International Journal of Information Management*, Vol. 54, p. 102152.

Maennel, K., Mäses, S. and Maennel, O. (2018), "Cyber hygiene: the big picture", *Nordic Conference on Secure IT Systems*, pp. 291-305.

Manjikian, M. (2018), *Cybersecurity Ethics: An Introduction*, Routledge, New York.

Marquardson, J. and Gomillion, D. (2018), "Cyber security curriculum development: protecting students and institutions while providing hands-on experience", *Information Systems Education Journal*, Vol. 16 No. 5, p. 12.

Mazar, N., Amir, O. and Ariely, D. (2008), "The dishonesty of honest people: a theory of self-concept maintenance", *Journal of Marketing Research*, Vol. 45 No. 6, pp. 633-644.

McNamara, T.P. (2005), *Semantic Priming: Perspectives from Memory and Word Recognition*, Psychology Press, London.

McNamara, A., Smith, J. and Murphy-Hill, E. (2018), "Does ACM's code of ethics change ethical decision making in software development?", *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, p. 729.

Mead, N.R., Gibson, D.S. and Hawthorne, E.K. (2015), "Cyber sciences and software engineering", *2015 IEEE 28th Conference on Software Engineering Education and Training*, pp. 21-23.

Minton, E.A., Cornwell, T.B. and Kahle, L.R. (2017), "A theoretical review of consumer priming: prospective theory, retrospective theory, and the affective–behavioral–cognitive model", *Journal of Consumer Behaviour*, Vol. 16 No. 4, pp. 309-321.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly*, Vol. 42 No. 1, pp. 285-311.

Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S. and Hancock, G.M. (2020), "Holistic cyber hygiene education: accounting for the human factors", *Computers and Security*, Vol. 92, p. 101731.

Nguyen, T. and Bhatia, S. (2020), "Higher education social engineering attack scenario, awareness & training model", *Journal of The Colloquium for Information Systems Security Education*, Vol. 8, p. 8.

Nyinkeu, N.D., Anye, D., Kwedeu, L. and Buttler, W. (2018), "Cyber education outside the cyberspace: the case of the catholic university institute of buea", *International Journal of Technology in Teaching and Learning*, Vol. 14 No. 2, pp. 90-101.

OpenUniversitiesAustralia (n.d), available at: https://www.open.edu.au/advice/insights/your-guide-to-university-as-a-mature-age-student

Pólkowski, Z. (2015), "Ethical issues in the use and implementation of ICT", *Sankalpa: Journal of Management and Research*, Khajuria, R., Banerjee, R. and Sinha, K. (Eds), *4th International Conference on 'Business Ethic for Good Corporate Governance and Sustainability'*, Ahmedabad, Gujarat Technological University, pp. 2-5.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders' motivation to protect organizational information assets", *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179-214.

Pournaghshband, V. (2013), "Teaching the security mindset to CS1 students", *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, pp. 347-352.

Raj, R.K., Blair, J.R., Sobiesk, E. and Parrish, A. (2018), "Enhancing cybersecurity content in undergraduate information systems programs: a way forward", *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy*, Vol. 1.

Rezaee, Z., Elmore, R.C. and Szendi, J.Z. (2001), "Ethical behavior in higher educational institutions: the role of the code of conduct", *Journal of Business Ethics*, Vol. 30 No. 2, pp. 171-183.

Richards, J.M. and Ekstrom, J.J. (2015), "The cyber education project and IT IAS curriculum", *Proceedings of the 16th Annual Conference on Information Technology Education*, pp. 173-178.

Richards, D., Formosa, P., Ryan, M., Hitchens, M. and McEwan, M. (2020), "A proposed AI-enhanced serious game for cybersecurity ethics training", *Conference of the Australasian Institute of Computer Ethics (9th: 2020)*, pp. 1-9.

Richardson, M.D., Lemoine, P.A., Stephens, W.E. and Waller, R.E. (2020), "Planning for cyber security in schools: the human factor", *Educational Planning*, Vol. 27 No. 2, pp. 23-39.

Rosenhan, D. (1972), "Learning theory and prosocial behavior", *Journal of Social Issues*, Vol. 28, pp. 151-163.

Rosoff, H., Cui, J. and John, R.S. (2013), "Heuristics and biases in cyber security dilemmas", *Environment Systems and Decisions*, Vol. 33 No. 4, pp. 517-529.

Ryan, M., Staines, D. and Formosa, P. (2017), "Focus, sensitivity, judgement, action: four lenses for designing morally engaging games", *Transactions of the Digital Games Research Association*, Vol. 2 No. 3, pp. 410-429.

Schlenker, B.R. (2008), "Integrity and character: implications of principled and expedient ethical ideologies", *Journal of Social and Clinical Psychology*, Vol. 27 No. 10, pp. 1078-1125.

Sefcik, L., Striepe, M. and Yorke, J. (2019), "Mapping the landscape of academic integrity education programs: what approaches are effective?", *Assessment and Evaluation in Higher Education*, Vol. 45 No. 1, pp. 30-43, doi: 10.1080/02602938.2019.1604942.

Sembok, T. (2004), "Ethics of information communication technology (ICT)", *Proceedings of the Regional Meeting on Ethics of Science and Technology*, pp. 239-325.

Sharma, K., Zhan, X., Nah, F.F.-H., Siau, K. and Cheng, M.X. (2021), "Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 1 No. 1, pp. 69-91, doi: 10.1108/OCJ-03-2021-0009.

Shieh, M. and Rajivan, P. (2021), "Influence of cumulative risk priming on security update decision making", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 65, pp. 353-357.

Singhapakdi, A. and Vitell, S.J. (2007), "Institutionalization of ethics and its consequences: a survey of marketing professionals", *Journal of the Academy of Marketing Science*, Vol. 35 No. 2, pp. 284-294.

Smith, C. (2018), "Cyber security, safety, & ethics education", Utica College.

Snyder, M.G. (2004), "Cyber-ethics: pirates in the classroom", *Science Activities*, Vol. 41 No. 3, p. 3.

Sobiesk, E., Blair, J., Conti, G., Lanham, M. and Taylor, H. (2015), "Cyber education: a multi-level, multi-discipline approach", *Proceedings of the 16th Annual Conference on Information Technology Education*, pp. 43-47.

studyanywhere (n.d), available at: https://studyanywhere.com.au/faq/student-visa-australia-age-limit

Tioh, J.-N., Mina, M. and Jacobson, D.W. (2019), "Cyber security social Engineers an extensible teaching tool for social engineering education and awareness", *2019 IEEE Frontiers in Education Conference (FIE)*, pp. 1-5.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. and Bailey, M. (2016), "Users really do plug in USB drives they find", *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 306-319.

Vallor, S. and Rewak, W.J. (2018), *An Introduction to Cybersecurity Ethics*, Santa Clara University, Santa Clara, CA.

Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G. and Chin, J. (2020), "Cyber hygiene: the concept, its measure, and its initial tests", *Decision Support Systems*, Vol. 128, p. 113160.

Woodward, B., Davis, D.C. and Hodis, F.A. (2007), "The relationship between ethical decision making and ethical reasoning in information technology students", *Journal of Information Systems Education*, Vol. 18 No. 2, pp. 193-202.

Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q. and Sprissler, E. (2018), "Finding the weakest links in the weakest link: how well do undergraduate students make cybersecurity judgment?", *Computers in Human Behavior*, Vol. 84, pp. 375-382.

Yoon, C. and Kim, H. (2013), "Understanding computer security behavioral intention in the workplace", *Information Technology and People*, Vol. 26, pp. 401-419.

Zhang, Y., Lin, H., Zhang, X. and Ye, Q. (2021), "The next steps in academic integrity—education, awareness, norms, duty and law", *Forensic Sciences Research*, Vol. 6 No. 4, pp. 341-346.

(The Appendix follows overleaf)

Appendix 1
Survey deployed on qualtrics

Part B-1: Demographics

Q1: What is your gender? Female, Male, Other

Q2: How old are you? ____

Q3: What cultural group do you most strongly identify with?

Oceania (including Australian)	
North-Western European	
Southern-Eastern European	
North African and Middle Eastern	
South-East Asian	
North-East Asian	
Southern and Central Asian	
People of the Americas	
Sub-Saharan African	
I don't identify with any cultural group	

Q4: What is your main area of study?

Psychology
Computing
Arts
Business
Other

Q5: How often do you use any of the following IT services and resources of XX University?

IT resources and services	1= Never, 2= Rarely, 3= Sometimes, 4=Often, 5=Everyday				
iLearn	1	2	3	4	5
XX Wi-Fi	1	2	3	4	5
XX Virtual Private Network (VPN)	1	2	3	4	5
XX Website	1	2	3	4	5
XX IT helpdesk	1	2	3	4	5
XX Library	1	2	3	4	5
XX Email	1	2	3	4	5
XX Licensed software (e.g. Office 365, Endnote)	1	2	3	4	5
Computer Labs	1	2	3	4	5

Part B-2: Scenarios

Version 1.1: A student enrols in a web design unit at XX University. While studying, they are also working for a company that builds commercial websites. Their employer has assigned them a project to build an eCommerce website. The student builds and tests the website on XX University servers which are accessible to students for their academic studies. The student continues to host the website on University servers when the site goes live to the public.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 2.2: A student has a full day of lectures to attend. After the first few hours they feel drained. During a break between classes, they decide to watch a show to refresh, but they realise that their personal data pack is about to run out. They decide to watch the show by logging onto and using the University's Wi-Fi network. Impressed with the speed of the internet, they log into their personal Netflix account and download at the lowest resolution one episode of their favourite show so that they can enjoy watching it when they get back home.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 3.1: A friend starts a new private company and is looking to hire students who will soon be graduating. They ask you to share with them an email list of all your fellow classmates so that they can publicise these job opportunities. In order to help them, you locate a mailing list on a University server and forward it to your friend. The list you forward to your friend contains the first names, last names and personal email addresses of all your fellow classmates. Using the data from the mailing list, your friend uses their company's network to start sending bulk personalised emails to all your fellow classmates advertising the job opportunities.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 4.2: A student finds a USB thumb drive unattended for a long time in one of the University's computer labs. Out of curiosity, since they are studying computer viruses as part of their university studies, they insert the thumb drive into one of the University's computers in the lab that is specifically setup for students to study the impacts of computer viruses. Once inserted, unknown software from the USB drive immediately starts installing onto the computer. This infects it with a virus and causes it to crash. The student uses a software package installed on the computer to successfully remove the virus and restore the system and learn about the impacts of the virus.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 5.1: A student uses the XX University network to download software for their project work from various third-party websites. The downloads include creative commons and pirated software. They complete their project with the downloaded software and submit it for assessment to their lecturer.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 1.2: A student enrols in a web design unit at XX University. While studying, they are also working for a company that builds commercial websites. Their lecturer has assigned the student a project to build an eCommerce website. The student builds and tests the website on XX University servers which are accessible to the students for their academic studies. The student continues to host the website on University server until their lecturer can assess it.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 2.1: A student has a full day of lectures to attend. After the first few hours they feel drained. During a break between classes, they decide to watch a show to refresh, but they realise that their personal data pack is about to run out. They decide to watch the show by logging onto and using the University's Wi-Fi network. Impressed with the speed of the internet, they log into their personal Netflix account and download at the highest resolution 10 seasons of their favourite show so that they can enjoy watching it when they get back home.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 3.2: A friend starts a new private company and is looking to hire students who will soon be graduating. They ask you to share with them an email list of all your fellow classmates so that they can publicize these job opportunities. In order to help your friend, you send the details of the employment opportunities to your fellow classmates so that they can send their contact details to the company if they are interested in applying. Using the data, they received from the students who directly contacted them, your friend uses their company's network to start sending bulk personalized emails to those students who contacted them advertising the job opportunities.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 4.1: A student finds a USB flash drive unattended for a long time in one of the University's computer labs. Out of curiosity, they insert the thumb drive into one of the University's computers in the lab. Once inserted, unknown software from the USB drive immediately starts installing onto the computer. This infects it with a virus and causes it to crash. They restart the machine even though the virus is still there to carry on with their assignment.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Version 5.2: A student uses the XX University network to download software for their project work from various third-party websites. The downloads include creative commons and proprietary software for which XX University has a license. They complete their project with the downloaded software and submit it for assessment to their lecturer.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree	Disagree	Somewhat disagree	Neither disagree nor agree	Somewhat agree	Agree	Strongly agree	No position / Refused
O	O	O	O	O	O	O	O

Why_____

Part-C 1: How good is your knowledge about the following:

Subjects	Terrible	Poor	Average	Good	Excellent
Information Technology (IT)	O	O	O	O	O
Using Computers	O	O	O	O	O
Cybersecurity	O	O	O	O	O
Ethics	O	O	O	O	O
Ethics in IT	O	O	O	O	O
XX University's Acceptable Use of IT Resources Policy?	O	O	O	O	O

Appendix 2

Scenario-pair version		G1 (17–20) 187 participants μ	SD	G2 (21–56) 73 participants M	SD	Independent samples T-Test p-value
1. Hosting a website	1.1	3.45	1.720	2.82	1.719	0.009*
	1.2	5.51	1.761	4.88	2.054	0.021*
2. Downloading series to watch	2.1	3.20	1.784	3.11	1.822	0.722
	2.2	4.39	1.698	3.67	1.732	0.003*
3. Sharing email list of fellow classmates to others	3.1	2.36	1.443	1.93	1.273	0.026*
	3.2	4.66	2.081	4.33	2.014	0.241
4. Inserting unattended USB into university computer	4.1	1.97	1.330	1.82	1.097	0.388
	4.2	3.58	1.871	3.67	1.965	0.736
5. Third party software download	5.1	2.94	1.838	2.81	1.680	0.592
	5.2	5.40	1.974	5.22	1.995	0.519

Note(s): *There is a significant difference at $p < 0.05$

Table A1. Result analysis of comparing scenario responses between age groups 17–20 and 21–56

Scenario-pair version		G1 (17–34) 239 participants μ	SD	G2 (35–56) 21 participants M	SD	Independent samples T-Test p-value
1. Hosting a website	1.1	3.41	1.734	1.71	0.784	<0.001*
	1.2	5.44	1.802	4.19	2.228	0.044*
2. Downloading series to watch	2.1	3.23	1.797	2.52	1.632	0.340
	2.2	4.31	1.697	2.71	1.488	0.092
3. Sharing email list of fellow classmates to others	3.1	2.29	1.425	1.67	1.065	0.070
	3.2	4.59	2.054	4.29	2.217	0.426
4. Inserting unattended USB into university computer	4.1	1.94	1.266	1.81	1.327	0.843
	4.2	3.65	1.857	3.14	2.287	0.065
5. Third party software download	5.1	2.98	1.811	2.05	1.322	0.037*
	5.2	5.44	1.937	4.33	2.198	0.109

Note(s): *There is a significant difference at $p < 0.05$

Table A2. Result analysis of comparing scenario responses between age groups 17–34 and 35–56

Corresponding author
Deborah Richards can be contacted at: deborah.richards@mq.edu.au