Routledge
Taylor & Francis Group

🔓 OPEN ACCESS | Check for updates

Using game-based learning to teach young people about privacy and online safety

Jane Henriksen-Bulmer [a], Emily Rosenorn-Lanng [b], Stevie Corbin-Clarke [b], Samuel Ware [a], Davide Melacca [a] and Lee-Ann Fenge [b]

[a]Department of Computing and Informatics, Bournemouth University, Fern Barrow, Poole, UK; [b]National Centre for Post-Qualifying Social Work, Bournemouth University, Fern Barrow, Poole, UK

ABSTRACT

Game-based learning can be a useful tool for increasing engagement in topics that are typically not related to games such as privacy and staying safe online, yet, very few games exist that look at how we can passively teach audiences how to stay safe online. This paper presents a bespoke board game about privacy, aimed at young people aged 16–25 years, to help them safely navigate the online world and understand the privacy consequences of their actions. Using a Case Study methodology, this paper covers the development of the prototype game, a Snakes and Ladders/ Trivial Pursuit style game about online scams, trolls, cyberbullying and other areas of digital safety. We also explain how the game questions were created, and the development and testing of the game itself. We trialled the game through a series of focus groups and found that young people passively learn how to stay safe online in a fun and interactive manner through playing the game. This makes the game an effective way to teach young people about the dangers of cyberspace in a safe, non-threatening manner, thereby demonstrating how an interactive game about digital privacy and online safety, can be used to more effectively protect young people from the many dangers of cyberspace.

1. Introduction

Young people use the internet as a primary method of communicating with each other to the extent that this is now for many how they experiment with their social identities and build relationships (Cardoso et al., 2019). Furthermore, smartphone ownership allows young people constant access to the internet, potentially putting them at risk of exposure to toxic content, exposure to harassment and data breaches (Mitchell et al., 2014). In 2018, Ofcom reported that 83% of 12–15-year-olds had their own smartphone and 71% of these were allowed to take their phone to bed, suggesting this is the preferred way for young people to access the internet (Ofcom, 2018).

Protecting young people's online interaction skills is about raising their awareness, as software and other measures can only do so much. Digital literacy, understanding privacy and resiliency are essential skills to ensure that young people have positive, educational, and fun experiences online (Mitchell et al., 2014).

CONTACT Jane Henriksen-Bulmer ✉ jhenriksenbulmer@bournemouth.ac.uk

In this paper, we present a privacy game that seeks to passively teach young people how to stay safe online. The team behind this project sought to fuse expertise from across the computing, gaming and health and social care sectors to "co-create" a gamification tool based on our current research into privacy risk (Henriksen-Bulmer et al., 2019), scamming and victimisation (Lee & Fenge, 2018; Rosenorn-Lanng et al., 2019). The output was a privacy game, a cross-between Trivial Pursuit (Haspro, 1999) and Snakes and Ladders, that uses game-based learning as a tool for raising awareness in young people about the dangers of sharing too much detail when online.

The rest of this paper is organised as follows. In Section 2, we provide a brief background review. In Section 3, the research questions (Section 3.1) and methodology (Section 3.2) are outlined, before describing how the game categories were devised in Section 4. We present the game design and prototype are presented in Sections 5 and 6; followed by the evaluation in Section 7, and discussion of findings in Section 8. Section 9 concludes the paper by answering the research questions, and discussing limitations (Section 9.1), and future work (Section 9.2).

2. Background

2.1. Privacy and safeguarding

Privacy to many is about protection our personal rights and, for some, protection of our right to a private life. This notion is depicted through Article 12 of the Universal Declaration of Human Rights (The General Assembly of the United Nations, 1948), and enacted into law through the European Convention of Human Rights which grants us; "the right to respect for his private or family life, his home and his correspondence" (Council of Europe, 1950). However, defining what that means in practice is perhaps a little more difficult. To illustrate, we each have different perceptions of what privacy might mean for us, for example, some consider privacy the ability to choose whether or not to participate (Parker, 1974), while others consider it a state of mind (Weinstein, 1971). Other scholars discuss privacy in terms of what harm may be done to us either personally or digitally, e.g. decisional interference or surveillance (Solove, 2006), or indeed the extent to which we have a right to influence how much information about us is/may be shared with others (Nissenbaum, 2010). Perhaps the broadest view is that privacy is a more fluid concept that encompasses everything from our personal boundaries to our role as 'self' and how we interpret the world around us, that changes over time as our perception alters (Palen & Dourish, 2003).

Safeguarding concerns ensuring vulnerable people (young and old) are safe and protected from harm (Fenge & Brown, 2017). This includes making sure those that are able understand how to protect themselves (Willoughby, 2019). This, by extension, includes ensuring they understand their privacy rights, how to enforce them, and what steps they can take to keep safe online.

2.2. Young people, privacy and online safety

Young people are increasingly using the internet and social media to communicate with each other, with 95% of 3-17 year olds using video-sharing or social media platforms and 62% also having their own profice (Ofcom, 2022). Other work has found that "the majority" of children in Europe engage in online social activity on a daily basis (Smahel et al., 2020). As part of this, young people may share private or confidential information with their peers, thereby increasing their risk of exposure to unwanted cyber aggression, cyber-bullying and potentially risky friendships (Goldstein, 2016). Moreover, lack of privacy awareness can lead to young people posting or falling victim to inappropriate postings, cyber-attacks (such as getting hacked), stalking or bullying (Martin et al., 2018).

Research has confirmed that nearly a third of young people have experienced hurtful, harmful or nasty content online (Ofcom, 2022a). As a result, online privacy is an increasing area of concern, particularly for young people, as their online activities increase. Research shows that children are starting to use electronic devices, social media, and the internet at large from younger and younger ages.

For example, in 2022, 62% of 8-17 year olds had more than one online profile, despite 58% of parents being aware that most social media platforms have a minimum age requirement of 13 years old (Ofcom, 2022).

Safeguarding young people online requires a comprehensive approach that includes education, training, and awareness-raising (El-Asam, Katz, Street, Nazar, & Livanou, 2021). This includes being aware of a wide range of online risks, such as cyberbullying, grooming, and exposure to harmful content (Lonergan, Moriarty, McNicholas, & Byrne, 2023). Prior and Renaud (2022) argue to reduce online vulnerabilities, children from all socio-economic backgrounds would benefit from an 'extra-curricular intervention program' to teach current password "best practice" and to support in embeddinga password management skill set.

The 2020 ChildFund rapid review, estimated that: 1.5 billion children were globally impacted by school closures and lockdowns, as a result of the Covid-19 pandemic (ChildFund, 2020). This led to a reported increase in cyberbullying, grooming and production of child sexual abuse material (Asam & Katz, 2018). The level of impact is variable, depending on the young person's personal circumstances and support network (Roehl & Stewart, 2018). Known impacts include: privacy interpretation, that may lead to over-sharing or over-exposure; online abuse and cyber-bullying, that can lead to anxiety and depression (Craig et al., 2020) and physical and mental health complaints (Giumetti & Kowalski, 2022); exposure to negative content such as that promoting self-harm, that could lead to a decreased sense of well-being; physical and mental health deterioration; heightened vulnerability to exploitation (Willoughby, 2019). Other risks, such as vulnerability to cyber-scams or sexual solicitation (DeMarco et al., 2017), could lead to fear; a personal violation; inability to replace lost funds, leading to financial anxiety, self-blame, embarrassment, shame or guilt e.g. if the young person thinks they contributed to the victimisation; and loss of trust or confidence in others – especially when the cyber-attacker is someone they have developed a "digital" relationship with. These events can have a negative impact on the cyber-victim's health and well-being, which can create societal costs by, for example, an increased need for mental or physical care or support (Asam & Katz, 2018; Rosenorn-Lang et al., 2019).

Some argue that it is up to the parents of these children to control their children's screen time and internet usage (Pardhan, Parkin, Trott, & Driscoll, 2022; Davies, Atherton, Calderwood, & McBride, 2019; Roehl & Stewart, 2018), however, parents often find this challenging and as a result, children inevitably end up online, unsupervised (InternetMatters, 2022). Thus, young people are unlikely to know how to protect themselves and their privacy online, and so, equipping young people with the knowledge, skills and understanding of the dangers and pitfalls of the internet is vital.

This project sought to address these challenges though the development of an educational game, aimed specifically at young people, to help them understand the privacy risks, how they may occur, and help them navigate through their online activities in a safe, privacy-preserving manner.

2.2.1. Categorising Privacy and Online Safety into Groupings

Looking at risk through a privacy lens, Finn, Wright, and Friedewald (2013) had categorised privacy into seven areas: privacy of association; privacy of location and space; privacy of thoughts and feelings; privacy of data and image; privacy of communication; privacy of behaviour and action; and privacy of the person, while Solove (2006) had created a taxonomy of 'harmful activities', whereby harm could be considered to fall under: information collection; information processing; information dissemination; or invasion of privacy.

Looking more specifically at children and privacy online, Livingstone, Stoilova, and Nandagiri (2019) conducted a study of growing up in a digital age. They found that children and young people's perception and appreciation of privacy develops as they grow, listing online privacy, location and data tracing, lack of understanding of what can go wrong, and understanding how

to protect themselves online, as some of the areas that young people may be unclear about. Thus, the next objective was to find studies that would more clearly list or identify these risks.

In this area, we found that Kaspersky (2020) had created a list of what they consider to be the top 7 dangers that children face online: cyber bullying; predators; posting private information; phishing; scams; malware; and old posts never go away.

Similarly, the UK Council for Internet Safety, developed a framework to equip children and young people for digital life. The framework outlines 8 areas that need to be addressed as part of any intervention: self-image and Identity; online relationships; online reputation; online bullying; managing online information; health, wellbeing and lifestyle; privacy and security; and copyright and ownership (UK Council for Internet Safety, 2020).

Ofcom (2022b) took a slightly dierent approach, categorising hams young people may encounter online into types; (1) Content Harm, such as exposure to negative self-image, sexual or self-harming materials; (2) Contact Harm, such as witnessing harmful behaviours or being bullied; and (3) Commercial Harms, such as scamming, misinformation or being put at risk from commercial collection of data. Further, in their 2023 Children and parents: media use and attitudes report, Ofcom had grouped harms into: wellbeing and safety; sharing of personal information online; exposure to age-inappropriate content; experiencing detriment or harm; and reputational damage (Ofcom, 2023).

Willoughby (2019), on the other hand, conducted a systematic review of the research around risks of young people's online interactions. From this he concluded that, while online social activity brings many opportunities to young people for sharing and networking, it also poses a number of potential risks. He categorised these risks into four categories: online abuse and cyberbullying; exposure to negative user-generated content; converging of on- and o-line worlds; and developing privacy interpretations.

2.3. Learning with games

Using games for learning encourages intrinsic motivation to learn, that has been shown to increase learning and provide a positive learning experience (Chan & Ahern, 1999). It is therefore not surprising that educational gaming is an area of substantial growth, especially digital game-based learning (Barseghian, 2012). Yet, very few games touch on the specific area of "privacy" that we are looking at. In creating a privacy game that is aimed initially at young people, we will endeavour to increase awareness of contextual privacy and highlight the privacy implications and risks of their digital footprint(s). The main aim will be to increase awareness and teach young people how to protect themselves better in an increasingly digital world.

Games are a fun way to learn and, as such, we believe can provide researchers and teachers with an opportunity to use games as tools to create powerful learning aids that, when done well, can turn "learning [into] the drug" (Koster, 2014).

2.3.1. Game-based learning
Game-based learning (GBL) and gamification are two approaches that have gained attention in the field of education for their potential to enhance engagement andlearning outcomes. GBL involves the use of games as educational tools, providing immersive and interactive experiences that promote active learning (Bellotti et al., 2013). In contrast, gamification is the process of applying game design in a non-gaming context (Deterding, Dixon, Khaled, & Nacke, 2011). GBL has emerged as a compelling educational approach that integrates games and learning processes to promote engagement and enhance educational outcomes (de Freitas, 2018; Ericksen, 2019; Jaaska and Aaltonen, 2022), whereas gamification is, arguably, more about driving behaviours to keep players to remain engaged through applying game elements, such as points, badges, and leaderboards, to non-game contexts to enhance motivation and engagement; focusing on incorporating game mechanics into educational activities to drive targeted behaviours (Plass,

Homer, & Kinzer, 2015). GBL also offers opportunities for learners to engage in problem-solving, critical thinking, and collaboration. Therefore, a GBL approach is best suited for a learning environment if the aim is to both increase engagement and ensure knowledge acquisition in a subject that is typically not related to games (Caponetto, Earp, & Ott, 2014). Studies have shown the positive impact of game-based learning on engagement, motivation, and learning outcomes across various disciplines (Chow, Woodford, & Maes, 2011; Flanagan & Nissenbaum, 2007; Pando Cerra, Fernandez Alvarez, Busto Parra, and Iglesias Cordera, 2022; Sousa & Rocha, 2019; Wu & Chen, 2010; Yuratich, 2021). Games can induce a state of flow by providing clear goals, immediate feedback, and a balance between challenge and skill, resulting in heightened motivation and learning (Kiili, de Freitas, Arnab, & Lainema, 2012). Flow Theory suggests that optimal learning experiences occur when individuals are fully immersed and engaged in an activity (Csikszentmihalyi, 1990).

With this project, the aim was to create an effective game in which the players would learn passively, meaning that the students would learn something about privacy, and how to protect themselves online, without necessarily realising they were learning. This way, young people are provided with an opportunity to learn by lack of privacy awareness, and provided with best practice advice for safeguarding their digital footprint, and preserving their privacy, in an interactive and safe way. Furthermore, the study sought to gain insight into young people's perspectives on digital privacy, that could be used to inform age-appropriate response techniques and advice for young people and professional practitioners working with young people on contextual privacy in a digital world. As young people are likely to have played and enjoyed games before, it may be beneficial to use games in the classroom to teach different subjects. This is because games can promote more engagement with a subject when the goal is not to only learn, but to potentially win. Therefore, games centred around important subjects can be a useful teaching tool (De Jans et al., 2017).

2.3.2. Existing privacy games

While educational gaming is a growing area (Caponetto et al., 2014), we only found one example of privacy being gamified in a card game designed to "as a political intervention" to help people make more informed privacy choices online (Barnard-Wills & Ashenden, 2015). However, the introduction of the General Data Protection Regulation (GDPR) (Parliament & the Council of Europe, 2018) means that some of the issues raised by the game may no longer be relevant or up to date.

3. Materials and methods

The project took the format of a case study, following Yin, with the unit of analysis being the young person, as they are the main subject of the study (Yin, 2013). As part of the case study, to demonstrate the quality of this research four types of validity checks were applied; construct, internal, external and reliability.

3.1. Research questions

The intention was to create a privacy game aimed at young people to inform and educate, through gamification and game-based learning, on the privacy risks associated with online activity and socialising. The intention was that the game would be created as a board game initially and loosely based on the Trivial Pursuit game (Haspro, 1999), with a view to later develop an online version for young people to play interactively. To this end, the case study sought to answer the following questions:

- **TP-RQ1**: What are the key aspects of privacy risks that young people need to understand in order to adequately protect themselves against negative impacts of their actions and interactions?

- **TP-RQ2**: What questions do we need to formulate within each of the key aspects identified in TP-RQ1 to maximise the understanding, knowledge transfer and retention of learning by game-players on each of these key areas? (Intended learning outcome 1 [ILO1])
- **TP-RQ3**: How can we impart knowledge and understanding of the privacy risks associated with online social interaction, through the use of gamification, to help young people understand?

3.2. Case study format

In order to answer the research questions the case study was divided into five work packages (WPs); Category and Question Design (WP1, Section 4); Game Design (WP2, Section 5); Create Game Prototype (WP3, Section 6; Game Evaluation via focus groups (WP4, Section 7); and Game Dissemination (WP5, Section 9.2).

4. WP1 - category and question design

Firstly, Work Package (WP) 1 involved identifying the categories that would be used as a basis for the game questions to be developed. Identifying these, would enable us to answer the first research question (TP-RQ1).

4.1. Identifying categories for the game

A literature review was conducted around privacy and online safety risks to young people in Section 2.2.1, to identify what the main areas of risk were for young people interacting online. From this, the following sets of potential lists of key areas that we could use to inform the game categories, were identified:

(1) Daniel Solove's (2006) taxonomy of four groups of `harmful activities': (a) Information collection; (b) Information processing; (c) Information dissemination; and (d) Invasion of privacy (Solove, 2006).
(2) Finn et al.'s (2013) research to distinguish seven types of privacy: (a) Privacy of association; (b) Privacy of location and space; (c) Privacy of thoughts and feelings; (d) Privacy of data and image; (e) Privacy of communication; (f) Privacy of behaviour and action; and (g) Privacy of the person.
(3) Kaspersky's Top 7 dangers that children face online: (a) Cyber bullying; (b) Predators; (c) Posting private information; (d) Phishing; (e) Scams; (f) Malware; and (g) Old posts never go away (Kaspersky, 2020).
(4) UK Council for Internet Safety: A framework to equip children and young people for digital life, a set of 8 aspects that educators should consider when teaching young people about online safety: (a) Self-image and Identity; (b) Online relationships; (c) Online reputation; (d) Online bullying; (e) Managing online information; (f) Health, wellbeing and lifestyle; (g) Privacy and security; and (h) Copyright and ownership (UK Council for Internet Safety, 2020).
(5) Ofcom's list of harms groupings: (a) Wellbeing and safety; (b) Sharing of personal information online; (c) Exposure to age-inappropriate content; (d) Experiencing detriment or harm; and (e) Reputational damage. (Ofcom, 2023).
(6) Willoughby's four categories of risk: (a) Online abuse and cyberbullying; (b) Exposure to negative user-generated content; (c) Converging of on- and off-line worlds; and (d) Developing privacy interpretations. (Willoughby, 2019).

Upon analysis of these groups, it was decided that, while Solove's taxonomy of privacy harms had effective groupings for privacy and data processing, there were not enough categories for a

functioning game. Furthermore, the research team agreed that these categories did not include all of the topics that were deemed important for young people to be educated on. Therefore, this grouping was discounted from the list. A further review of all of the groupings was carried out, in order to map them against each other, and identify commonalities and similarities (Figure 1).

Figure 1. Game category mapping.

From there, definitions were agreed and a final list of categories were derived for the game, these were: Managing your information; Self-identity & Well-being; Cyber bullying & Trolling; Your relationships and reputation; and Privacy and Security (Figure 2).

Thus, the first research question was answered (TP-RQ1), and the key privacy risks that young people need to understand in order to adequately protect themselves against negative impacts of their actions and interactions were established: Managing your information; Self-identity & Well-being; Cyber-bullying & Trolling; Relationships and reputation; and Privacy & Security.

4.2. Designing Questions for the Game

The second research question (TP-RQ2, Section 3.1) required the development of a set of questions for each of the identified 5 game categories, that would facilitate young people to improve their understanding, knowledge transfer and retention of learning" [ILO1] in each of the identified categories. These questions would need to be informed by the literature and organised in grouping based on the five categories identified for the game (Section 4.1, Figure 2). Thus, each member of the research team was assigned a category to formulate a set of questions for, based on the findings of the Prolific survey (Section 4.2.1) and best practice from the literature.

4.2.1. Prolific survey

To inform the questions and gain insight into the end user's understanding of each of the categories within the game, we carried out an online survey using the Prolific platform (Prolific, 2020). This survey was anonymous, and was designed to establish what the primary areas of concern around privacy online are for young people, parents and guardians, and those who work with young people (teachers, youth workers, etc.). A link to a copy of the survey questions asked can be accessed via (https://doi.org/10.6084/m9.figshare.23726121).

Figure 2. Young People's Confidence in managing own privacy online.

As part of the survey, we collected general demographic information and consent from from all participants, explaining that no personal data about them would be collected. The survey itself asked 75 questions around privacy and gaming to establish preferences and opinions. All participants were asked to give consent We surveyed 90 adults, parent guardians and those who work with young people aged 14–25 in the UK ("educators"), and 91 young people (aged 18–25).

4.2.1.1. How young people interact online. Looking at the young people (63% male, 37% female respondents) specifically, we found that the most popular online activity that young people engage with online daily is Social Media (91.2% accessed Social Media on a daily basis), closely followed by socialising via direct messaging (86% used direct messaging every day). This corresponds with Ofcom's findings that children and young people regularly use the internet and social media to communicate with each other (Section 2.2).

4.2.1.2. Young People's confidence levels in each of the Game Categories. The young people were asked how concerned they were in relation to the different categories of risks identified in the literature (Section 2.2.1). The results showed that the primary areas of concern for young people were: privacy and security; phishing and scams; and location tracking (Figure 3), and so it was vital that these areas of concern would be covered as part of the privacy and security category within the game.

4.2.1.3. Young people and privacy. The young people were asked how confident they were in managing their online privacy and the responses suggest that, while most knew how to access and change their privacy settings, many did not check or alter these setting on a regular basis (see Figure 4).

4.2.1.4. Using games for education. Analysis of the adult responses found that 65% had concerns about the online privacy of the young people they interact with (see Figure 5), demonstrating the need for more education in this area.

Which category would you say you are most concerned about?

Category	Value
Self-image and identity	15 (16.5%)
Online relationships	1 (1.1%)
Online reputation	2 (2.2%)
Online bullying/ Cyber bullying / In-game bullying	3 (3.3%)
Managing online information	8 (8.8%)
Health, well-being, and lifestyle	2 (2.2%)
Privacy and security	30 (33%)
Copyright and ownership	0
Scams and phishing	21 (23.1%)
Location tracking	9 (9.9%)
Safety settings	0
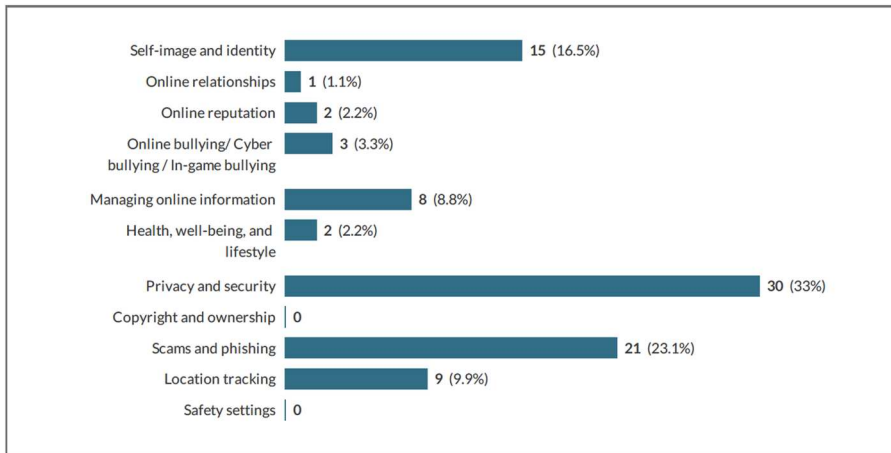
Figure 3. Categories of concern for Young People.

I regularly check and update my privacy settings

Strongly Agree	9 (9.9%)
Agree	29 (31.9%)
Neither	17 (18.7%)
Disagree	34 (37.4%)
Strongly Disagree	2 (2.2%)
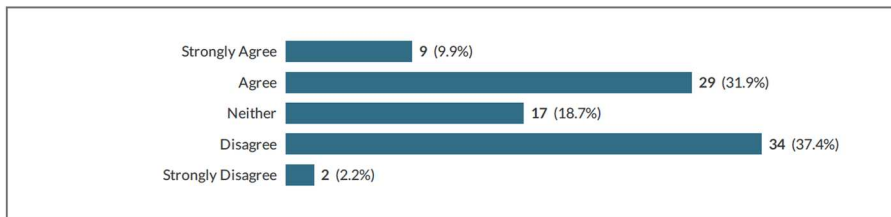
Figure 4. Young People's Confidence in managing own privacy online.

I worry about the digital privacy of some of the young people I work or live with

Strongly Agree	17 (18.9%)
Agree	48 (53.3%)
Neither	12 (13.3%)
Disagree	11 (12.2%)
Strongly Disagree	2 (2.2%)
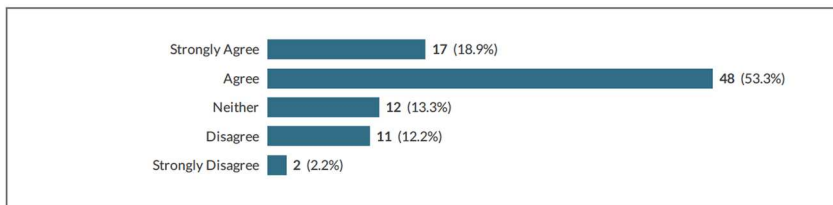
Figure 5. Educator's perception of young people's digital privacy.

When we asked the adults (which included parents, educators and guardians) whether they have used or would use an educational board game to support learning of the young people they interact with, more than three quarters (78%), would use this type of game in their interactions with young people (see Figure 6).

4.2.1.5. Educators Perception of Risk for young people online. Upon being asked about their main areas of concern for young people navigating online (the same question asked to the young people (Figure 3), the adults' biggest concern was cyber bullying (Figure 7). In contrast, young people rarely rating it as an area of concern (3% for young people vs 39% educators). Data analysis revealed that

Educational board game
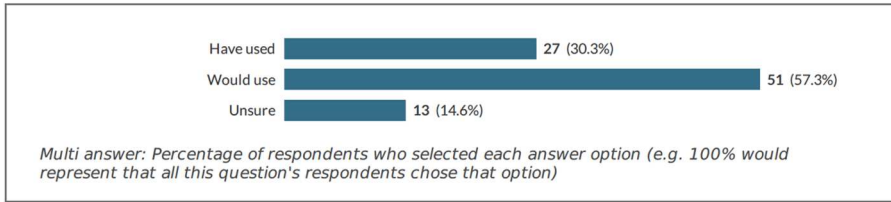
Figure 6. Educator's usage of Educational Board Games.

parents and guardians were mostly concerned about online bullying, sexual predators, privacy and protecting personal information, with regards to the young people they interact with (Figure 7). Young people (18–21-year-old) were also concerned about their privacy and protecting their personal information (Figure 3). However, there was little in the data to suggest they were concerned with cyberbullying and sexual predators. They were far more worried about hacking and hackers, which is a subject the parents and guardians did not frequently report as a key area of concern.

which one you are most concerned about.

Figure 7. Categories of concern for Educators.

4.3. Game questions

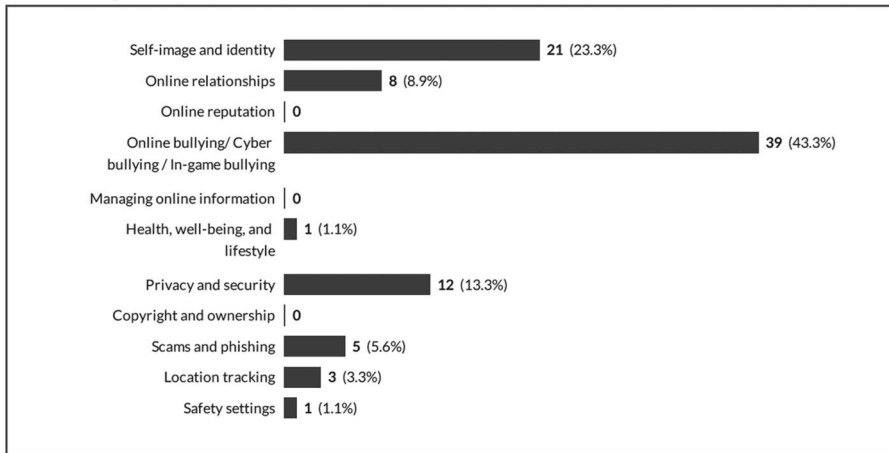Information gathered from the Prolific survey acted as a starting point for informing the questions (Prolific, 2020). For example, the survey asked adults what aspects of a game they felt should be considered to ensure the game would be as accessible to as many young people as possible. Out of the 86 answers received, the most frequent answers were that the game should be fun (28 mentions), easy to play, and not too complicated (14 mentions). Thus, a second intended learning outcome [ILO2], *to assess ease of use and fun as a metric for the success of the design*.

From the survey results, the concerns raised were organised into the five categories to ensure they were reflected within the game; this means that the question subjects were informed by people's real-world concerns with online privacy and safety. Consequently, this would help to ensure learning within the game would have real-world relevance to the players.

For example, in the area of Privacy and Security, concerns raised from the Prolific survey revealed that phishing, scams and location tracking were areas of particular concern for young people (Section 4.2.1.2). Thus, questions were included that covered these topics as part of the question

design (Table 1). To also reflect the literature and adults' concern around cyber bullying (Section 4.2.1.5), we also made sure to include questions around this area within the game (Table 2).

Table 1. Example game questions.

Question	Answer choices
What is an online troll?	(a) A character from Lord of the Rings (b) A mythical character (c) Someone who deliberately tries to sabotage your game or upset you (d) A glitch in your computer
How can you check your social media privacy settings work?	(a) Go onto another device and look at your social media from there (b) Hope for the best (c) You can't (d) Ask a friend

Table 2. Example Game Questions – Cyber Bullying.

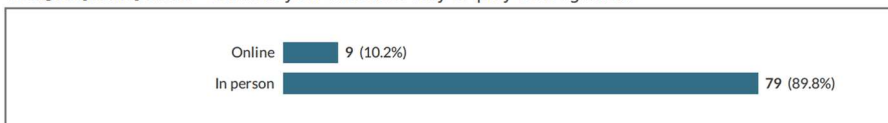| Question	Answer choices
What is an online troll?	(a) A character from Lord of the Rings. (b) A mythical character (c) Someone who deliberately tries to sabotage your game or upset you. (d) A glitch in your computer.

5. WP2 - game design

Work Package 2 sought to answer the third research question and design the physical game. For this, a Scrum agile approach was used; a method based on iterative cycles designed to support and facilitate continual incremental improvements being made to the design, throughout the process, known as "Sprints" (Schwaber & Sutherland, 2020).

There are a couple of ways to turn a subject into a game. The first is to adapt the subject directly into game mechanics. For example, a mathematics game may involve solving problems within a certain time frame to beat enemies. Another method involves implementation of a quiz-style format. The mechanics of a quiz-style game would include delivering players questions and providing immediate feedback, including positive reinforcement and reward when a player answers a question correctly and encouragement or an explanation when a player answers incorrectly. Quizzes can cover a wide variety of topics and there is software than can make inserting or updating questions neither complicated, nor time-consuming. This makes it an ideal method of gamification. Kahoot is an example of a popular quiz game that is used in education to promote active learning (Jones et al., 2019).

5.1. Physical or digital?

In the survey, participants were asked whether they felt a physical or digital boardgame would be preferred by young people. The responses from the adults showed that almost half (43 out of 90) had a preference for physical board games and 42 showed a preference for digital board games (5 did not respond), indicating a balance between the two. However, young people themselves overwhelmingly elected they would prefer a physical board game to an online one (Figure 8).

Figure 8. Young People Response to whether they preferred physical or online board game.

5.2. Question Cards

The first sprint (Schwaber & Sutherland, 2020) in the iterative Scrum process sought to design a physical solution that would allow players to answer the questions created. (Section 4.3). A set of game cards were designed for the questions to be input into (Figure 2). The purpose of the questions is to encourage and stimulate conversation between players, as the educational nature of the answers is of benefit to all players. The question cards were printed out to form a deck (e.g. Figure 9), including a clearly distinct question set for each category, thereby answering the second research question (TP-RQ2).
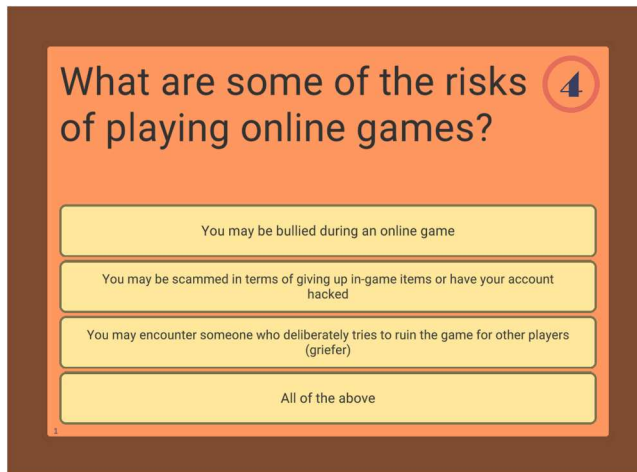

Figure 9. Example game card.

6. WP3 - game prototype

The second sprint involved developing the mechanics of the game and what elements should be included in the game to make it effective, interactive and fun to play. When participants were asked what they believed were the most important aspects to consider when designing a game for educational purposes. The most frequent responses were that the game should be fun and relevant to the players, easy to use and accessible, in terms of catering for diversity in players' skills andabilities [ILO2]. Educational games combine learning with play (Prensky, 2003), aiming to create a learning environment that is fun and safe, two attributes that respondents stated were important. Thus, having devised the questions, focus moved towards the mechanics of the game and ensuring the game was not overcomplicated and the rules were straightforward and possible to grasp the first time it is played.

To support the main function of the game, which is the answering of questions, other mechanics had to be designed with this in mind. This means that the game mechanics should not be at odds with each other, or take the focus away from the main core game mechanic.

6.1. Game rules

In sprint 3, a rule book was created to support and guide gameplay. The rule book takes the form of a small, A5 booklet, and explains the rules of the game (Figure 10), as well as the different components of the board (Sections 6.2 to 6.4).
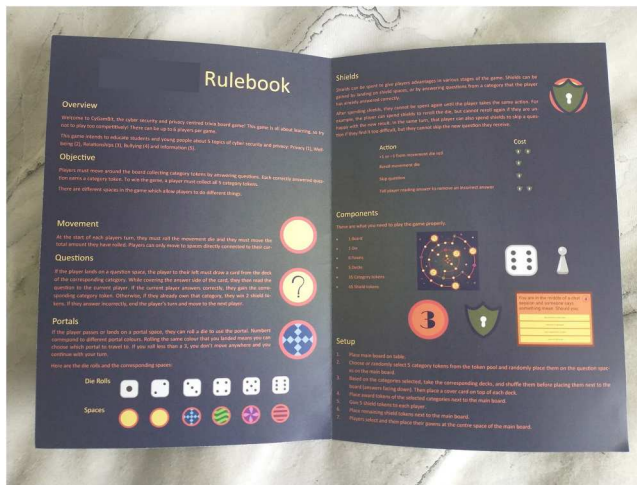
Figure 10. Rule Book.

6.2. Portals

The game takes inspiration from the board games of Snakes and Ladders and Trivial Pursuit. Drawing from the concept of players sliding up or down the board when they land on a snake or ladder (Snakes and Ladders), the idea of portals that allow players to reach questions in different areas of the board more easily, without having to use a turn, was developed. However, unlike in Snakes and Ladders, this mechanic only serves to benefit the player and not a punishment. This maintains a sense of unpredictablity and interactivity, whilst allowing players to reach questions faster.

6.3. Tokens

Inspired by the concept of collecting "wedges" in Trivial Pursuit (Haspro, 1999), the idea of collecting "trophies" was introduced as part of the game design. For this, category tokens were designed; these tokens demonstrate that you have proven your knowledge in one of the privacy categories. Players can acquire a category token when answering a question from that category correctly. Shield tokens were also introduced; these tokens can be used to modify die roll results to reach questions faster, and/or to assist in answering questions, by removing two of the answers (Figure 11).

Figure 11. Category tokens above and a shield token below.

6.4. Game board

The game board was designed in a circle shape, with players being able to move in any direction on the board, allowing them to move more freely towards whichever category they require a token for. An illustration of the game board can be found in Figure 12.
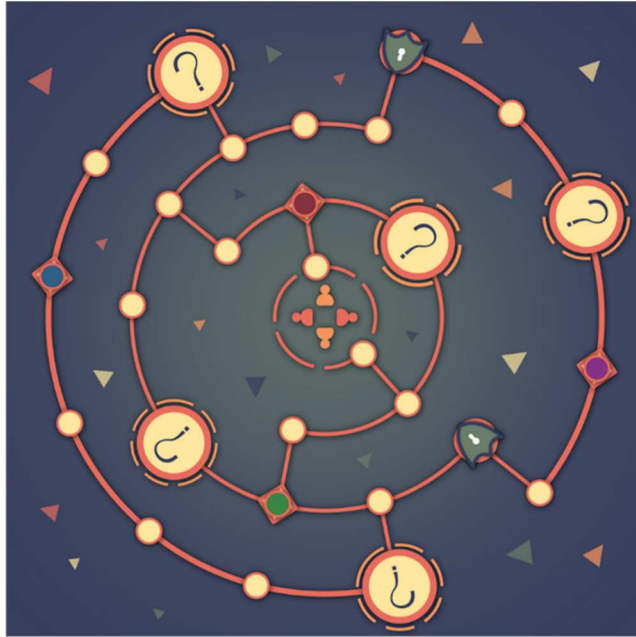
Figure 12. Game Board Design.

7. WP4 - game evaluation

The final work package (WP4) involved evaluating the game with end users (young people). For this purpose, sprint 4 involved combining all the game components into a paper prototype of the game. This involved printing out all of the game elements which included the game board; the 5 decks of questions (one for each category); the tokens and shields; and the rule book. Some dice and playing pieces were also sourced to allow users to play. The purpose of creating the paper prototype was to gain feedback and uncover any issues with the game, to aid improvents in the future. To evaluate the game, it was first important to establish whether the ILOs had been achieved. To do this, the effectiveness of the questions and whether they achieved the intended learning outcomes needed to be tested (TP-RQ2; to improve "the understanding, knowledge transfer and retention of learning by game-players" [ILO1] in each of the identified categories) (TP-RQ1, Section 3.1). Secondly, testing needed to be carried out to ensure the game was easy to use, accessible and fun to play [ILO2] (Section 4.3).

7.1. Trialling the game

In total, we had 27 young people take part in trialling the paper prototype. The trials took place in a focus group setting with teams of 4–5 undergraduate students aged between 18 and 25 being asked to participate and play the game.

All players were asked to complete a pre-game questionnaire before the trial began. This pre-game questionnaire asked about their perception and level of confidence around each of the 5 game categories (Figure 2).

Players were then divided into groups of 4–5 players, provided with an overview of the rules the game and invited to each select a unique playing piece (Figure 13).

Figure 13. First paper prototype being tested in a focus group of students.

8. Results

After each group had completed their game, the players were asked to complete a post-game questionnaire, including 15 rating questions, to explore their experience with playing the game. This included questions about their perceptions of privacy, as well as some usability questions (based on the System Usability Scale by John Brooke (Brooke, 1996), and questions relating to their experience of the play session and game design.

The evaluation questionnaires were designed using Likert scale ranking, which meant that each question could include multiple layers. For example, Q9 was devised with the intention of obtaining participants' feedback on the gameplay experience (Figure 14), but also enabled the collection of feedback relating to the participants' perceptions of the difficulty level of gameplay, as well as their thoughts and opinions on the questions in the game.
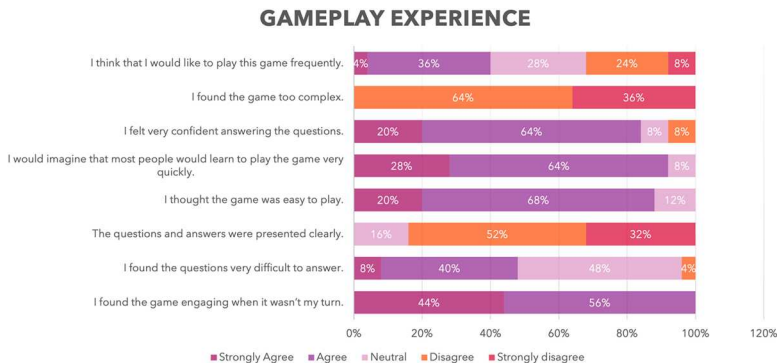
Figure 14. Evaluation Questionnaire.

8.1. Learning

Upon analysing the results of the evaluation questionnaires, it emerged that all players reported feeling more confident across all 5 game categories as a result of playing the game (Figure 15). This exceedingly positive response suggested that the first learning outcome [ILO1] had been achieved.

Figure 15. Player's Confidence Levels.

Although some of the levels of improvement were slight (ranging from $1 - 13$ percent improvement), this could indicate that the level of questions are better suited to the younger end of the chosen demographic, rather than those at the higher end of the age group. This was also commented on by one of the players who stated: "*It was engaging, especially for a younger audience*" (P7). However, due to COVID-19 restrictions and limited access to younger participants (players), this was not possible to test.

To assess learning, the self-rated scores of each of the five question categories (see Figure 2) from the pre-game questionnaires and the post-game questionnaires the Wilcoxon (1945). Test found an improvement in knowledge across all the categories.The most significant gains were seen in the "managing your information" and "your relationships and reputation" categories ($p < 0.01$). Other significant positive shifts were recorded in relation to the "cyber-bullying and trolling" and "self-identity and well-being" categories ($p < 0.05$). This may indicate that those aspects are more difficult for young people to navigate and therefore, further exploration may be needed into how best to continue increasing awareness in those areas.

The questionnaires were completed immediately prior to and immediately after gameplay, which indicates that any significant differences observed within the group, between these two points, can be directly attributed to the gameplay experience and demonstrated the efficacy of the game as an effective learning tool. Overall, players were in agreement that the game was easy to play, and was not too complex (Figure 14). This indicates that the design goal of making an intuitive game [ILO2] was achieved, which developed from Section in which 14 participants in the Prolific survey shared that they felt an educational game should be easy to use. Whilst playing the game, the majority of groups engaged in informal debates and discussions about the questions and their potential answers; this was the case both for their own questions and those of other players. This acts to reinforce the passive learning element for all players. Respondents were also in agreement that the questions and answers were presented clearly, and reported that they came away from the experience feeling they had learnt something about their online privacy from playing the game (Figure 17), confirming that the game meets the [ILO1], set out in Section 3.1.

These findings, coupled with the fact that we asked the questions both before game play and immediately after play, support the argument that any significant differences observed within the group, between these two points, can be directly attributed to the gameplay experience. thereby demonstrating the efficacy of the game as an effective learning tool (Figure 13).

Overall, players were in agreement that the game was easy to play, and that the game was not too complex (Figure 14). This relates back to Section 4.2.1 where 14 prolific participants thought that an educational game should be easy to use [ILO2]. This means we achieved our design goal of making a game that is easy to use and intuitive. We found that, while a couple of the groups simply played the game, reading and answering the questions, most had discussions around potential answers for each question even if the question was not theirs. This was exactly what we had hoped would happen as this will reinforce the passive learning element for all players. After finishing the game, players were also mostly in agreement that the questions and answers were presented clearly and reported that they came away from the experience feeling they had learnt something about their online privacy from playing the game (Figure 16), thus confirming that the game meets the first learning outcome, set out in Section 3.1 [ILO1].
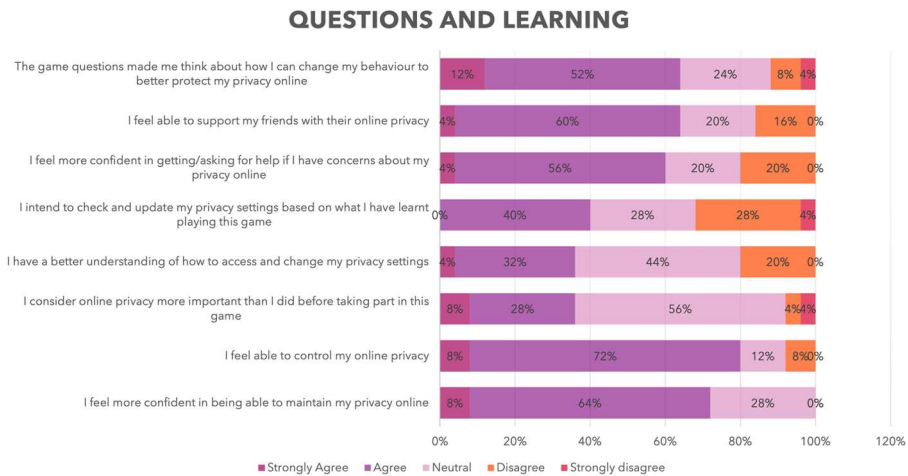
Figure 16. Reaction to Online Privacy post play.

9. Conclusion

This project aimed to create an interactive board game, which would serve to teach young people about digital privacy and how to stay safe when navigating online. To this end, we asked three questions; "*What are the key aspects of privacy risks that young people need to understand in order to adequately protect themselves against negative impacts of their actions and interactions?* (TP-RQ1); "*What questions do we need to formulate within each of the key aspects identified in TP-RQ1 to maximise the understanding, knowledge transfer and retention of learning by game-players on each of these key areas?*" (TP-RQ2); and "*How can we impart knowledge and understanding of the privacy risks associated with online social interaction, through the use of gamification, to help young people understand?*" (TP-RQ3).

These questions were answered through 5 work packages, the first of which looked to answer TP-RQ1 Section 3.1, by reviewing the literature around privacy and young people to establish the key areas that we needed to cover within educators around their privacy and gaming understanding and preferences. From this, in the second work package, the feedback from the Prolific surveys, combined with the literature was used to create question sets for each of the 5 categories identified for use within the game, thereby answering question TP-RQ2 (Section 3.1).

In work package 3, a prototype game board (Section 6), that was used to evaluate the game, as part of work package 4 (Section 7). The evaluation consisted of 4 focus groups, involving 27 participants playing the game. The feedback was positive, with responses confirming that the questions were thought-provoking, and encouraged learning and a change in behaviour when navigating online (Section 8, Figure 12).

Moreover, this work has demonstrated how play can be effectively way to facilitate passive learning about privacy in young people, thereby showing gamification and game-based learning are excellent tools for disseminating learning material to young people. Hence, the evaluation answered research question 3 by demonstrating that; "*knowledge and understanding of privacy risks associated with online social interaction… [can be imparted through gamification] to help young people understand*" [TP-RQ3].

9.1. Limitations

The Covid-19 pandemic meant that the original plan to develop a digital game and trial it with various age-groups within the chosen demographic was not possible. The majority of educational institutions were closed, meaning that access to younger participants proved problematic and therefore, the initial evaluation focus group sessions were limited to the young people that were most easily accessible to the project team (i.e. Bournemouth University students) to evaluate the game (Section 8).

9.2. Future work

Future work will look at how best to disseminate the game (the objective of work package 5). As part of this, further focus group sessions will be conducted, including younger players and the educators, to diversify the perspectives acquired. In relation to the game design, work has begun to develop an interactive digital version of the game, that players can access via the internet. It will also look to revise and update the question set, to expand and cover additional demographics and ensure learning remains current. In the longer term, additional question-sets will introduce other relevant topics around cyber security and privacy. The sets will be interchangeable, to suit both different learning needs and demographics e.g. elderly people, young people, etc. and the versatility of this framework will ensure that learning remains tailorable to different demographics.

Ethics

This study was conducted following ethical guidelines for research and full ethics approval was sought and granted from the University Ethics Committee prior to commencing research on this project (Rowley, 2002; Yin, 2013).

Notes on contributors

Dr Jane Henriksen-Bulmer is an experienced business analyst and Principal Academic in Computer Science based in the Department of Computing & Informatics at Bournemouth university. Her research is primarily concerned with Privacy by Design techniques and tools. She brings a significant amount of experience to the team having carried worked on a number of research projects that worked with various groups around privacy education and awareness.

Emily Rosenorn-Lanng is a Research Project Officer and Part-Time PhD candidate, based within the National Centre for Post-Qualifying Social Work at Bournemouth University. Currently undertaking a PhD is Game-Based Learning in Social Work Higher Education, Emily is an experience quantitative researcher, having undertaken a wider portfolio of research projects within the academic and social research sectors.

Stevie-Corbin-Clarke is a full-time Research Assistant based within the National Centre of Post-Qualifying Social Work. Stevie is a qualified teacher, specialising in working with young people. Stevie is an experience qualitative researcher, having undertaken a wide portfolio of research projects with marginalised and hard to reach groups.

Samuel Ware is a full-time Technical Research Assistant – based within the Department of Computing & Informatics. Samuel supports all areas of technical development of the game. Experienced in developing games, frameworks and apps, Samuel acts as the primary interface for all technical aspects of the project.

Davide Melacca is a part-time Technical Research Assistant – based within the Department of Computing & Informatics. Davide brings a unique combination of technical skills and game design experience to the team. Having played a key role in developing a number of immersive simulation and game-based experiences for the social work sector in both digital and physical formats.

Lee-Ann Fenge is Professor of Social Care in the Faculty of Health and Social Sciences. She is a Registered Social Worker and has always been committed to advancing the professional evidence base of social care practitioners.

ORCID

Jane Henriksen-Bulmer http://orcid.org/0000-0002-0807-2661
Emily Rosenorn-Lanng http://orcid.org/0000-0002-0481-4517
Stevie Corbin-Clarke http://orcid.org/0000-0003-0223-7979
Samuel Ware http://orcid.org/0009-0002-5466-5887
Davide Melacca http://orcid.org/0009-0008-6022-9743
Lee-Ann Fenge http://orcid.org/0000-0003-0896-7323

References

Barnard-Wills, D., & Ashenden, D. (2015). Playing with privacy: Games for education and communication in the politics of online privacy. *Political Studies*, *63*(1), 142–160. https://doi.org/10.1111/1467-9248.12049

Barseghian, T. (2012). Explosive growth in education apps. KQED: Mind Shift.

Bellotti, F., Kapralos, B., Lee, K., Moreno-Ger, P., & Berta, R. (2013). Assessment in and of serious games: An overview. *Advances in Human-Computer Interaction*, *2013*, Article 136864. https://doi.org/10.1155/2013/136864

Brooke, J. (1996). Usability evaluation in industry. In *chap. SUS: A quick and dirty usability scale*. Taylor Francis.

Caponetto, I., Earp, J., & Ott, M. (2014). Gamification and education: A literature review. In *Proceedings of the 8th European Conference on Games-Based Learning ECGBL 2014* (Vol. 1, pp. 50–57).

Cardoso, P., Hawk, D. V., & Cross, D. (2019). What Young people need to make better-informed decisions when communicating with digital images: Implications for mental health and well-being. *Health Education & Behavior*, *47*(1), 29–36. https://doi.org/10.1177/1090198119885433

Chan, T. S., & Ahern, T. C. (1999). Targeting motivation – adapting flow theory to instructional design. *Journal of Educational Computing Research*, *21*(2), 151–163. https://doi.org/10.2190/UJ04-T5YB-YFXE-0BG2

ChildFund. (2020, April). *Rapid review of online safety risks: Full report* (Tech. Rep.). Child Fund Alliance: Young and Resilient Research Centre [online].

Chow, A. F., Woodford, K. C., & Maes, J. (2011). Deal or no deal: using games to improve student learning, retention and decision-making. *International Journal of Mathematical Education in Science and Technology*, *42*(2), 259–264. https://doi.org/10.1080/0020739X.2010.519796

Council of Europe. (1950, Nov). *European convention on human rights, as amended by protocols nos. 11 and 14* (Tech. Rep.). Council of Europe [online].

Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., Harel-Fisch, Y., Malinowska-Cieślik, M., Gaspar de Matos, M., Cosma, A., Van den Eijnden, R., Vieno, A., Elgar, F. J., Molcho, M., Bjereld, Y., & Pickett, W. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, *66*(6), S100–S108. http://doi.org/10.1016/j.jadohealth.2020.03.006

Csikszentmihalyi, M. (1990, 01). *Flow: The psychology of optimal experience*. New York: Harper and Row.

Davies, S. C., Atherton, F., Calderwood, C., & McBride, M. (2019, Feb). *Uk chief medical officers' advice for parents and carers on children and young people's screen and social media use*. Online.

de Freitas, S. (2018). Are games eective learning tools? a review of educational games. *Journal of Educational Technology and Society*, *21*(2), 74–84.

De Jans, S., Van Geit, K., Cauberghe, V., Hudders, L., & De Veirman, M. (2017). Using games to raise awareness: How to co-design serious mini-games?. *Computers & Education*, *110*, 77–87. https://doi.org/10.1016/j.compedu.2017.03.009

DeMarco, J. N., Cheevers, C., Davidson, J., Bogaerts, S., Pace, U., Aiken, M., . . . Bifulco, A. (2017). Digital dangers and cyber-victimisation: A study of European adolescent online risky behaviour for sexual exploitation. *Clinical Neuropsychiatry*, *14*(1), 104–112.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "Gamification". In *Proceedings of the 15th international academic mindtrek conference: Envisioning future media environments* (pp. 9–15). Association for Computing Machinery. https://doi.org/10.1145/2181037.2181040

El Asam, A., & Katz, A. (2018). Vulnerable young people and their experience of online risks. *Human–Computer Interaction*, *33*(4), 281–304. http://doi.org/10.1080/07370024.2018.1437544

El-Asam, A., Katz, A., Street, C., Nazar, N. M., & Livanou, M. (2021). Children's services for the digital age: A qualitative study into current procedures and online risks among service users. *Children and Youth Services Review*, *122*, 105872. http://doi.org/10.1016/j.childyouth.2020.105872

Ericksen, K. S. (2019). Educational instruction for group work with diverse members: Innovative student classroom engagement using a game-based learning activity. *Currents in Teaching and Learning*, *11*, 67–78.

Fenge, L.-A., & Brown, K. (2017). *Safeguarding adults: Scamming and mental capacity*. Sage.

Finn, R., Wright, D., & Friedewald, M. (2013). European data protection: Coming of age. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Poullet, (Eds.), (pp. 3–32). Springer.

Flanagan, M., & Nissenbaum, H. (2007). *A game design methodology to incorporate social activist themes*. Proceedings of the 2007 Conference on Human Factors in Computing Systems, CHI 2007, San Jose, CA, USA, April 28–May 3, 2007 (pp. 181–190).

The General Assembly of the United Nations. (1948, December). *The universal declaration of human rights* [online]. Retrieved April 29, 2017, from http://www.un.org/en/universal-declaration-human-rights/

Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. *Current Opinion in Psychology*, *45*, 101314. http://doi.org/10.1016/j.copsyc.2022.101314

Goldstein, S. E. (2016). Adolescents' disclosure and secrecy about peer behavior: Links with cyber aggression, relational aggression, and overt aggression. *Journal of Child and Family Studies*, *25*(5), 1430–1440. http://doi.org/10.1007/s10826-015-0340-2

Haspro, (1999). Trademark and copyright information. Horn Abbot Ltd and Horn Abbot International Ltd. https://www.hasbro.com/home/copyrightold.html.

Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2019). Privacy and identity management. Fairness, accountability, and transparency in the age of big data. In E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, & S. Krenn (Eds.), *privacy and identity 2018. IFIP advances in information and communication technology* (Vol. 547, pp. 173–188). Springer.

Internet Matters. (2022, June). *Insights from internet matters tracker survey* [online]. Retrieved 14 Apr 2023, from https://www.internetmatters.org/wp-content/uploads/2022/10/Internet-Matters-Insights-Tracker-June-2022.pdf

JŁaŁaskŁa, E., & Aaltonen, K. (2022). Teachers' experiences of using game-based learning methods in project management higher education. *Project Leadership and Society*, *3*, 100041. https://www.sciencedirect.com/science/article/pii/S2666721522000011

Jones, S. M., Katyal, P., Xie, X., Nicolas, M. P., Leung, E. M., Noland, D. M., & Montclare, J. K. (2019). A "KAHOOT!" approach: The effectiveness of game-based learning for an advanced placement biology class. *Simulation & Gaming*, *50*(6), 832–847. https://doi.org/10.1177/1046878119882048

Kaspersky, (2020). Internet safety for kids: How to protect your child from the top 7 dangers they face online. Retrieved March 1, 2022, from https://www.kaspersky.co.uk/resource-center/threats/top-seven-dangers-children-face-online.

Kiili, K., de Freitas, S., Arnab, S., & Lainema, T. (2012). The design principles for flow experience in educational games. *Procedia Computer Science*, *15*, 78–91. https://www.sciencedirect.com/science/article/pii/s1877050912008228 (4th International Conference on Games and Virtual Worlds for Serious Applications(VS-GAMES'12)).

Koster, R. (2014). *A theory of fun for game design [electronic resource]*. O'Reilly.

Lee, S., & Fenge, L. A. (2018). Scamming: Recognising and supporting victims of financial abuse. *Journal of Community Nursing*, *31*(6), 59–64.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age* [online]. London School of Economics and Political Science.

Lonergan, A., Moriarty, A., McNicholas, F., & Byrne, T. (2023). Cyberbullying and internet safety: a survey of child and adolescent mental health practitioners. *Irish Journal of Psychological Medicine*, *40*(1), 43–50. http://doi.org/10.1017/ipm.2021.63

Martin, F., Chuang, W., Petty, T., Weichao, W., & Wilkins, P. (2018). Middle school students' social media use. *Journal of Educational Technology & Society*, *21*(1), 213–224.

Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2014). *Trends in unwanted online experiences and sexting* (Tech. Rep.). University of New Hampshire: Crimes Against Children Research Centre.

Ofcom (2018). Children and parents: Media use and attitudes report.

Ofcom. (2022a, Mar). *Children and parents: media use and attitudes report* [online]. Author.

Ofcom. (2022b, June). *Online nation report 2022* [online]. Author.

Ofcom. (2023). *Children and parents: media use and attitudes report* (Tech. Rep.) [online]. Author.

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 129–136). New York, NY, USA: ACM. http://doi.acm.org/10.1145642611.642635

Pando Cerra, P., Fernandez Alvarez, H., Busto Parra, B., & Iglesias Cordera, P. (2022). Effects of using game-based learning to improve the academic performance and motivation in engineering studies. *Journal of Educational Computing Research*, *60*(7), 1663–1687.

Pardhan, S., Parkin, J., Trott, M., & Driscoll, R. (2022). Risks of digital screen time and recommendations for mitigating adverse outcomes in children and adolescents. *Journal of School Health*, *92*(8), 765–773. http://doi.org/10.1111/josh.v92.8

Parker, R. B. (1974). A definition of privacy. *Rutgers Law Review*, *27*(2), 275–297.

Parliament, E., & the Council of Europe (2018). *General data protection regulation (GDPR)* (Tech. Rep.).

Plass, J. L., Homer, B. D., & Kinzer, C. K. (2015). Foundations of game-based learning. *Educational Psychologist*, *50*, 258–283.

Prensky, M. (2003). *Digital game-based learning* (No. 1). ACM Computers in Entertainment.

Prior, S., & Renaud, K. (2022). The impact of financial deprivation on children's cybersecurity knowledge & abilities. *Educational and Information Technologies*, *27*, 10563–10583.

Prolific (2020). Prolific platform. Retrieved from https://prolific.co/.

Roehl, A., & Stewart, A. H. (2018). Impact of social networking sites and digital applications upon teens. *Journal of Family & Consumer Sciences*, *110*(2), 37–42. https://doi.org/10.14307/JFCS110.2.37

Rosenorn-Lanng, E., Corbin-Clarke, S., Lee, S., Forster, S., & Maskall, P. (2019). *Cyber fraud and scamming – guidance and advice* (Tech. Rep.). Bournemouth University: National Centre for Post-Qualifying Social Work. https://ncpqsw.com/publications/the-language-of-scams/.

Rowley, J. (2002). Using case studies in research. *Management Research News*, *25*(1), 16–27. https://doi.org/10.1108/01409170210782990

Schwaber, K., & Sutherland, J. (2020). The scrum guide: The definitive guide to scrum: The rules of the game. ScrumGuides.org.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Olafsson, K., Livingstone, S., & Hasebrink, U. (2020). *Eu kids online 2020: Survey results from 19 countries* (Vol. [online]; Tech. Rep.). EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. https://doi.org/10.2307/40041279

Sousa, M. J., & Rocha, Á. (2019). Leadership styles and skills developed through game-based learning. *Journal of Business Research*, *94*, 360–366. http://doi.org/10.1016/j.jbusres.2018.01.057

UK Council for Internet Safety (2020). *Education for a connected world: A framework to equip children and young people for digital life* (Tech. Rep.). UK Council for Internet Safety (UKCIS). [online].

Weinstein, M. A. (1971). The uses of privacy in the good life. *Privacy: Nomos XIII*, 94.

Wilcoxon, F. (1945). Individual comparisons by ranking methods. *Biometrics Bulletin*, *1*(6), 80–83. https://doi.org/10.2307/3001968

Willoughby, M. (2019). A review of the risks associated with children and young people's social media use and the implications for social work practice. *Journal of Social Work Practice*, *33*(2), 127–140. https://doi.org/10.1080/02650533.2018.1460587

Wu, W.-H., & Chen, W.-F. (2010). *Developing a game-based learning environment in classrooms: A conceptual model*. Society for Information Technology & Teacher Education International Conference. Association for the Advancement of Computing in Education (AACE).

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.) SAGE.

Yuratich, D. (2021). *Ratio! A Game of Judgment* : using game-based learning to teach legal reasoning. *The Law Teacher*, *55*(2), 213–226. http://doi.org/10.1080/03069400.2020.1773677