Informatics in Education, 2025, Vol. 24, No. 3, 617–643

DOI: 10.15388/infedu.2025.19

Competence-Based Informatics Education: Addressing Digital Challenges through the Prioritization of Threats

Julian TAUPE, Rainer W. ALEXANDROWICZ, Andreas BOLLIN, Peter SCHARTNER

Klagenfurt am Wörthersee, Universität Klagenfurt, Austria
Universitätsstraße 65/67, 9020
e-mail: jutaupe@edu.aau.at, rainer.alexandrowicz@aau.at, andreas.bollin@aau.at, peter.schartner@aau.at

Received: January 2025

Abstract. Integrating the understanding of digital threats into informatics education is crucial for preparing pupils to navigate the complexities of the digital world. This study provides foundational insights for embedding digital safety competencies within informatics curricula by prioritizing key threats faced by young people. Through data collected from 708 teachers and 278 parents in Austria, the study employs correspondence analysis to rank threats, including harmful content, data security, social risks, and online addiction. The findings highlight how these prioritized threats can inform the design of competence-based curricula, fostering computational thinking, data literacy, and ethical decision-making in pupils. This research bridges the gap between informatics education and digital safety, offering practical implications for educators and curriculum developers worldwide.

Keywords: Digital Threats, Research in Informatics Education, Digital Safety Education.

1. Introduction

Education is a powerful tool for shaping the future, and the integration of information and communication technologies is changing how we teach and learn. This makes computer science increasingly important in educational curricula – worldwide. However, the intensive use of digital media and related technologies have introduced significant challenges, such as handling digital distractions, addressing cyber mobbing, and the changing way teachers and pupils communicate with each other. It has become quite likely for young people being involved in cybercrime incidents, as highlighted by Europol (2024). According to Külling *et al.* (2022), more than a third of the 12- to 19-year-old surveyed said they had at least once been told something offensive or false about them in

private chats. Moreover, 50 % of young people of the same age indicate they had already received online contact requests with sexual intentions. Despite growing demand, current frameworks – such as the K-12 Computer Science Framework by K-12 Computer Science Framework Steering Committee (2016) – lack the specificity needed to guide teachers in addressing digital threats effectively.

This lack of clarity poses significant challenges for teachers, who must decide which competencies are most important to protect young people. The rapid development of digital technologies makes it hard for teachers to stay up-to-date with their knowledge, so a prioritization would be very helpful.

In the field of digital safety, there is one study where Taupe *et al.* (2025) categorize digital threats that can lead to physical, psychological, social or material damage. That study surveyed teachers who shared their experiences on digital threats for children and teenagers. To overcome the one-sided teacher perspective, this study also surveyed parents to capture their insights on threats faced by children and teenagers. To gain even deeper insights, we planned a study to survey pupils. However, due to necessary questions in regards of some of the digital threats and the fear of triggering trauma, approval from the responsible ethics committee could not be obtained to conduct the survey. Consequently, we decided to proceed without surveying pupils at this time. With this approach we aim to create a holistic understanding of digital threats, ensuring that the findings support improving how we learn and teach in an educational context. To find out which digital threats are the most pressing and where to start in teaching, the following research question is answered:

> *What prioritization can be taken for digital threats in the field of digital safety, when considering both parents' and teachers' perspective?*

By answering this question and ranking digital threats for young people from the perspective of teachers *and* parents, we aim to provide a basis for a dedicated competency model that helps teachers prioritize competencies to better protect pupils. Among other things, improved competency development in the field of digital safety contributes to transcending geographical boundaries and cultural divides, as it equips children and teenagers with competencies to navigate diverse online environments, engage respectfully across cultures, and protect themselves in global digital interactions. This trend has also affected children and teenagers, not just in Austria, but globally. We expect that the findings of this study provide universality in the patterns of young people being confronted with digital threats as perceived by parents. Even if patterns differ, these insights have the potential to inform and trigger similar research efforts elsewhere.

The remainder of this paper is structured as follows: Section 2 examines related publications and studies regarding threats in the area of digital safety as well as competencies. In section 3, previously defined categories and respective digital threats are briefly described. Section 4 describes the study conducted with parents in Austria – this includes the study setup, information about the questionnaire, applied methods and information of the earlier study with teachers. The findings of the parent study are

shown in section 5. Section 6 discusses and analyzes the study results followed by section 7 providing recommendations regarding competencies for the most relevant digital threats. Section 8 highlights thoughts on validity. Finally, section 9 presents conclusions and the future research direction.

2. Related Work

Our research revealed a large number of publications and projects focusing on digital threats or risks as well as opportunities. Some of these are presented below as examples.

Eichenberg and Auersperg (2018) list opportunities resulting from digital media and technologies and associated risks. They use a taxonomy of five areas of risks, which was initially proposed by Eichenberg and Kühne (2014): excessive, dysfunctional, self-damaging, deviant, and youth-endangering usage. Within these they discuss possible threats, and possible causes. Also, Gasser *et al.* (2012) discuss various digital threats young people are exposed to. Examples are cyberbullying, sexting, sexual harassment, and addictive behavior. They emphasize the key role of parents and teachers regarding the support of children and teenagers by actively participating in prevention and intervention to counter such threats. O'Keeffe *et al.* (2011) address issues caused by media-sharing platforms (like Facebook, Twitter, or YouTube). Interestingly they discuss not only risks like cyberbullying or sexting, but also possible advantages like socialization, communication and learning opportunities. Tintori *et al.* (2023) focus on topics such as grooming and cyberbullying. Inter alia, they point out how young people are vulnerable to grooming due to factors like low self-esteem, lack of social support as well as insufficient knowledge about possible risks of such approaches. In the course of the *EU Kids Online 2020* study, Smahel *et al.* (2020) cover the European perspective on digital risks and opportunities children and teenagers are facing. The study covers topics such as cyberbullying, sexting, online addiction, and identity issues. It highlights how young people use digital technologies to create and communicate their digital identities. Taupe *et al.* (2023, 2025) gathered digital threats potentially leading to physical, psychological, social, or material damage, forming the four categories "Content Harmful to Young People", "Social Environment", "Data, Data Protection and Information" and "Online Addiction". They found that 71 % of teachers in Austria have already experienced or witnessed at least one incident of young people having been confronted with a digital threat.

Looking at curricula in various countries reveals regional differences regarding digital competencies, sometimes split alongside federal states (e. g., Germany or Switzerland), sometimes managed centrally (e. g., Austria). Moreover, in Austria the so-called *Digital Basic Education* has been introduced in the 2022/23 school year as a mandatory subject in the curriculum for lower secondary school by the ministry of education, Bundesministerium für Bildung, Wissenschaft und Forschung (2023a,b). Competencies covered by this subject are defined in *DigComp 2.2 AT*, published by the ministry

for digital and economic affairs in Austria, Bundesministerium für Digitalisierung und Wirtschaftsstandort (2021). DigComp 2.2 AT is the Austrian version of the European competencies model *DigComp 2.2*, published by Carretero *et al.* (2017). The subject is mandatory in classes 5 to 8 (lower secondary school), with a minimum of one hour per week in the timetable. The competencies defined therein cover media usage and participation in the media culture, developing computational skills as well as communication, collaboration, critical thinking and problem-solving skills. The K-12 Computer Science Framework Steering Committee (2016) developed the *K-12 Computer Science Framework*. This framework provides guidelines for integrating computer science education into school curricula, but it is too general to help teachers communicating competencies in regards of digital threats.

Łukasz Tomczyk (Tomczyk, 2018) focuses on analyzing digital competencies from the parents' perspective in a population of parents of pupils in secondary schools in Poland. The objective of the study was to diagnose the level of digital competencies of parents regarding using digital media, focusing on six key areas of digital threats (ability to evaluate the correctness of information, interacting with other users safely, image protection on the Internet, respecting copyright, knowledge about cyberbullying, and using digital financial services). One conclusion is that parents start to realize that it is essential to improve their knowledge regarding digital technologies and their respective threats. Similarly, Arifin *et al.* (2019) conducted a study with parents of children under 18 in Malaysia. The authors report that parental awareness of the digital threats is at a medium level and requiring further improvement. They highlight the importance of parents' part supporting children and teenagers developing competencies specific to digital threats. Łukasz Tomczyk and Potyrała (Tomczyk and Potyrała, 2021) bring out parents' intuitive strategies for online safety of their children, which might not be the best at all. According to their study, parents often overestimate their digital literacy, so that their control measures may not ensure safe behavior. The results suggest that parents at least require knowledge to ensure basic protection against digital threats. The study further suggests that preventive programs should guide parents on modeling behaviors, promoting activities and fostering children's critical thinking. This is vital for shaping their digital awareness from early childhood on.

Currently, detailed data regarding online threats for children are not collected by authorities. Since parents and teachers serve as persons of trust for pupils in primary and secondary school, they are key to gaining more information regarding such threats. Teachers report that they have experienced or witnessed young people actually being involved to threats in the field of digital safety. Furthermore, there are only a few competencies defined in various curricula for primary and secondary school. Teachers' insight on threats that imperil children and teenagers in this realm is a unique perspective. The work of Taupe *et al.* (2023, 2025) thoroughly lists possible digital threats and reports on teachers' experience. It is is limited to this single perspective, which makes further research necessary to improve the situation in the educational context. The present study focuses on the perspectives and experiences of parents to enable a comprehensive view. We surveyed parents in Austria to obtain a final ranking of digital threats, providing a basis for future improvements in the classroom.

3. Background

The aim of this paper is to provide a prioritization of digital threats in the field of digital safety. Such threats have already been identified and gathered from various publications and grouped into four comprehensible categories. Parents have a different, equally important, relationship to children and teenagers when it comes to digital safety. By considering both perspectives, from teachers and parents, a comprehensive prioritization of digital threats can be developed. We follow the taxonomy of Taupe *et al.* (2025) grouping digital threats into four categories: *Content Harmful to Young People, Data, Data Protection and Information, Social Environment and Online Addiction*.

3.1. *Content Harmful to Young People*

This category deals with threats related to inappropriate content or products that target children and teenagers. Examples include the exposure to, creation, and distribution of illegal or inappropriate content as well as purchasing illegal substances online. These threats involve the potential exposure to or involvement with materials or products that are supposed to be illegal, harmful, or morally questionable for children or teenagers.

Illegal Content: Certain content may violate laws in different countries. According to Eichenberg and Auersperg (2018), an example for such content is *child pornography*. The federal criminal police office in Austria, Bundesministerium für Inneres, Bundeskriminalamt (2023), as well as Europol (2024), indicate that the spread of child pornography has been increasing in recent years.

Inappropriate Content: Questionable content is not illegal per se, but has the potential to harm others. Smahel *et al.* (2020) mention *cyberhate*, which includes hateful statements, mostly with an ethnic or religious background. Gasser *et al.* (2012) indicate that by using the Internet, young people have access to pornographic content and content that glorifies violence. Children and teenagers do not necessarily have to search specifically for them. Certain search terms can be used to accidentally find named material and subsequently consume it. Glaser *et al.* (2010) mention other examples like political campaigns, racism and other forms of discrimination.

Purchase Illegal Substances: Exposure to, or illegal acquisition of illegal substances is made easier by using the Internet. Eichenberg and Auersperg (2018) state that in addition to illegal drugs, this also includes medicines and their misuse.

3.2. *Data, Data Protection, and Information*

This category focuses on threats related to data and personal information. These threats can lead to data or privacy breaches, identity theft, financial loss, and impact decision-making processes and beliefs.

Personal Privacy: Smahel *et al.* (2020) mention posting an image of a person that is hurtful or hostile. Another example is using information about an individual in a way that the individual did not want. Also, the publication of the address or telephone number of another person on social media or other networks is an example.

Data Breach: Protecting data from unauthorized access is an important and sometimes difficult task. Aigner *et al.* (2020) and Drechsler *et al.* (2019) focus on various aspects. On the one hand there are attacks that take place in the context of social engineering, on the other hand there are threats of a technical nature such as viruses, trojans or similar that can lead to unauthorized access by third parties. Examples are fake e-mails with phishing links as well as the use of insecure passwords and hacker attacks.

Computer/Data Damage: Aigner *et al.* (2020) mention viruses and other computer programs that damage data or paralyze entire computers, as well as so-called ransomware. Ransomware are special programs that are used to specifically encrypt data so that it can no longer be used. Extortion attempts are usually behind it, in which the data is decrypted again in return for payment. Along with these threats, there are also peripherals such as USB devices that can physically damage a computer when plugged into it. Drechsler *et al.* (2019) highlight that social engineering also plays a role in this area. In many cases, technical attacks exploit human error, such as clicking malicious links, using weak passwords, or ignoring security warnings, which can directly lead to the compromise or loss of data.

Fake Information: This threat deals with information that is knowingly false or not factually substantiated. Eichenberg and Auersperg (2018) mention the phenomenon *cyberchondria*. This means that children and teenagers, among others, look for health symptoms primarily on the Internet before talking about them with trusted or knowledgeable people like doctors. This can lead to wrong and frightening conclusions which then may lead to other problems. Koerrenz and Diergarten (2022) highlight that *fake news* is one of the major issues young people have to cope with in the 21st century. False or alternative information exists in many areas. Such information is spread for different reasons. Examples are entertainment, conspiracy theories or even political influence.

Information Overload: Too much information, like spam or too many different sources of information, can lead to increased stress level. This includes difficulties in selecting information on the Internet. Eichenberg and Auersperg (2018) note that a high volume of e-mails, as well as researching for a presentation or the like, can already stress children and teenagers.

Reputation: Based on Palfrey and Gasser (2008), Gasser *et al.* (2012) point out that children and teenagers in particular are shaped by their digital identity. The digital identity is formed by all information about a person that can be found on the Internet. Protecting someone's *reputation* online is essential. A person's reputation can be damaged, for example, by distributing defamatory photos or videos on social networks. Smahel *et al.* (2020) mention that even parents can become perpetrators. Photos of children or teenagers are often published on the Internet, for example via WhatsApp status, Facebook, Instagram, or similar services, without their consent.

3.3. *Social Environment*

This category highlights threats arising from social interactions that can adversely affect children and teenagers. It encompasses behaviors like cyber mobbing, cyber stalking, trivialization of serious issues, online or offline contact with strangers, cyber grooming, and encouragement of violent or criminal activities. These threats can have profound emotional, psychological, and social consequences.

Cyber Mobbing: O'Keeffe *et al.* (2011) describe this threat as bullying in the digital context where false or damaging information about other people is spread through the use of digital technologies or media. Smahel *et al.* (2020) include statements in direct messages or social networks that are insulting or hurtful to someone.

Cyber Stalking: As stated by Eichenberg and Auersperg (2018), *cyber mobbing* describes the execution of activities in connection with stalking using technical means of communication such as smartphones or the Internet. The peculiarity of this type of stalking is that it is easier for attacks to hide their identity. Smahel *et al.* (2020) indicate that technologies such as GPS offer the possibility of determining the location of a person's smartphone.

Happy Slapping: Based on the Council for Crime Prevention in Schleswig-Holstein (2007), Gasser *et al.* (2012) describe this threat as having fun while punching someone. Attackers are often young and arbitrarily or purposefully look for a victim who is humiliated, tormented, beaten, raped, or otherwise abused. The act itself is filmed by the attackers or their accomplices and then distributed via various channels. Smartphones and the Internet make it easier to carry out, as they can be used to create the material and distribute it. The goal is not necessarily the act itself, but the resulting recognition and sense of power that comes with disseminating the act.

Injury Trivialization: In this collection, threats that lead to physical injuries are brought together. The basis of such threats is, among other things, the use of relevant social networks that speak positively about problematic issues. Eichenberg and Auersperg (2018) name suicide forums or pro-ana forums as examples. In these forums, those affected do not just try to help each other. Groups that downplay or even positively highlight the effects of such mental disorders also contribute to such networks.

Contact Strangers: Young people get to know new people online and sometimes meet them later in real life. Smahel *et al.* (2020) state there is also the opportunity for children and teenagers to get in touch with people who have bad intentions. Tintori *et al.* (2023) name *cyber grooming* as an example of such bad intentions. Adults try to contact children online and use manipulative communication to bring them to a meeting in the real world to ultimately sexually abuse or exploit them. Since the age of victims is steadily decreasing, research into the spread of this threat among primary school students is also necessary.

Violence/Crime Incitement: This collection bundles several digital threats. Gasser *et al.* (2012) define the term *sexting* as a combination of sex and texting. This means sending or receiving messages or media with a clearly sexual reference via digital devices. O'Keeffe *et al.* (2011) state that one of the main problems with this is that these messages can spread quickly over various networks. Smahel *et al.* (2020) mention that in general, sexting can also be seen as an opportunity to exchange wanted messages, but unwanted messages with this reference predominate. Girls and older children are particularly affected. Eichenberg and Auersperg (2018) point out *dares*, where young people can force others to take appropriate actions in order to be socially accepted. Such dares can be potentially risky and can lead to dangerous situations or injuries.

3.4. *Online Addiction*

This category encompasses threats related to addictive behaviors. These threats involve engaging in online activities that can have adverse effects, such as excessive online shopping leading to financial problems and impaired decision-making, gaming addiction characterized by excessive video game playing, and excessive use of chat forums and social networks resulting in prolonged online communication.

Online Shopping: Online shops offer advantages as well as disadvantages. Eichenberg and Auersperg (2018) state that the fact that these are practically always available can encourage addiction-like behavior in this area. Case studies show that excessive use of online shops can also lead to financial problems such as excessive instalment payments. In addition to classic consumer goods, Smahel *et al.* (2020) mention so-called in-app purchases, which can also lead to excessive spending. These in-app purchases can be found in apps as well as in games.

Gaming Addiction: Following Cypra (2005), Gasser *et al.* (2012) describe *gaming addiction* as the overuse or excessive use of computer games. Such behavior can be seen in offline as well as online games. This includes violent games, strategy games as well as massively multiplayer online role-play games. Eichenberg and Auersperg (2018) also state that computer games can be consumed on many platforms. Examples are computers or laptops, tablets, smartphones and also game consoles.

Social Media: Smahel *et al.* (2020) found that social networks as well as chat forums are already used by children and teenagers to communicate in different ways and to exchange diverse content. In most European countries, more than half of all children and teenagers use social networks on a weekly basis. Eichenberg and Auersperg (2018) also indicate that it is important to consider the potential dangers such as the emergence of addiction-like usage behavior. Individuals who particularly benefit of online communication are at increased risk of encountering such issues. It is of significant importance to pay due attention to these aspects.

4. Study

This report shows the findings of an empirical study surveying parents in Austria from January 22nd to March 11th 2024. We collected data from 278 parents across Austria in regards of how parents perceive digital threats in the field of digital safety.

4.1. *Questionnaire*

The questionnaire covered questions about demographics, how parents use digital media and parents' experience on digital threats for children and teenagers. That way, we want to find out how parents perceive digital threats and how they assess the relevance of these threats. The survey comprised closed-ended questions (single-choice, multiple-choice and value sliders) as well as ranking tasks. The complete questionnaire is available online on the website of the SecComp4All project[1] at the University of Klagenfurt.

4.2. *Population and Sampling*

The target population of this study was parents in Austria. Since it was not possible to directly sample parents, they have been contacted through parent associations – this encloses all parents of children and teenagers in primary and secondary school. In Austria there is an umbrella organization for parents' associations[2]. This organization provides contact data for each federal state's parents' association. All of these were asked to contact their associated parent associations to send an invitation to participate in the study directly to the parents. Other parent associations in Austria (e. g., the umbrella association of independent parent-child centers in Austria or Verein Einzigartig), which also operate across several federal states, were contacted with the same request. All education directorates in the federal states confirmed that surveying parents about their experience via parents' associations does not require any approval. To share the invitation to the study, umbrella organizations of parents' associations were asked to distribute the link to the study. These organizations either sent the invitation directly to parents or their associated parent associations. Ultimately, the link to the survey was distributed via channels the respective organization uses to communicate with parents. Some used social media, while others used e-mail, messaging services or apps used by schools. The focus was not to reach both parents of each pupil, but to encourage as many different parents as possible to take part.

[1] https://www.aau.at/en/informatics-didactics/research/projects/seccomp4all

[2] https://www.elternverein.at

4.3. *Survey*

The survey was realized as an online survey. Based on a pilot-study, we set the final wording and explanation of each of the questions. No incentives (e. g., gifts or similar rewards) were offered to participants to discourage perfunctory or insincere responses. Rather, we tried to motivate parents participating in the study, we emphasized the importance of the topic in the letter of information provided with the link to the survey. In contrast to the previously conducted study with teachers, the decision was made to remove the digital threat "Copyright" from this study. The reason for removing this threat is that, from the perspective of teachers, this threat does not seem to be relevant for young people. The figure showing the result of the correspondence analysis in the teacher study indicates, compared to all other evaluations, this threat is completely separate from the rest of the threats. One reason for this could be that, in contrast to other threats, the threat "Copyright" does not have any comparable, noticeable consequences for children or teenagers. This does not implicate that respecting copyright is not important.

4.4. *Methods*

The data presented in this manuscript result from the parents' survey, conducted as part of a larger research project that also included a survey of teachers. The teachers' dataset was analyzed and published in a previous paper by Taupe *et al.* (2025). Building on those published findings, the present work not only provides a detailed analysis of the parents' responses but also integrates them with the earlier teacher results to enable a comprehensive assessment of both groups.

Apart using common tools of descriptive statistics visuals are also used: Box and whisker plot, bar chart and tables. Values are rounded to a reasonable number of decimals. When specifying average values, the standard deviation is always specified as well.

Furthermore, we applied a correspondence analysis to work out the structure of the rankings. As described by Little (2013), correspondence analysis is a multivariate statistical technique and used for visualizing and describing the associations between multiple variables (in our case threats and ranks). It is especially useful for categorical data like counts or percentages. The main goal is to illustrate the specific association of the rows and columns of a data matrix as points in a spatial representation. In this study, the association between threats and a particular rank is not exclusively determined by how often that threat appears in a specific rank. Rather, the joint distribution of threats and ranks is considered to calculate the associations. Furthermore, the association of a threat with a certain rank is determined by various factors. These factors include the shared variation in the data as well as the relative positioning of threats and ranks in the analysis. This is a noticeable advantage compared to solely using relative frequency as a reference. When evaluating the ranking of threats correspondence analysis was used in favor of relative frequency. Herewith it was possible to visualize and interpret the complex associations between threats and ranks in a more comprehensible way. When

using relative frequency, each threat would have a percentage value for each rank, but it would not be easy to visualize and analyze influences of the different ranks on a threat. For this study, the data for correspondence analysis consisted of a contingency table in which each row represented one of the identified digital threats and each column a rank position. The cells contained the frequency with which a given threat was assigned a particular rank across all participants. Correspondence analysis decomposed this table into dimensions that capture the maximum variance in the joint distribution, allowing threats and ranks to be represented in a common two-dimensional space. The spatial proximity between a threat point (blue) and a rank point (red) in the resulting plot indicates a connection between them which is stronger than the average. This visualization enables the identification of patterns that are less evident in purely percentage-based comparisons – such as clusters of similar threats or ranks that tend to be associated with certain types of threats.

4.5. *Ranking by Teachers*

In a previous study, ranking of the aforementioned digital threats has been done by teachers. Therefore, teachers were asked to rank digital threats in terms of their relevance for young people. This intermediate result was discussed by Taupe *et al.* (2025) and is later used in developing a prioritization of digital threats. Additional results of the teacher study are values regarding teachers' first-hand experience with digital threats as described by Taupe *et al.* (2023). This means teachers experienced first-hand that young people have been confronted with digital threats. Table 1 shows the previously published ranking of threats by teachers – within their respective category. Multiple ranks may show a notable association with a single threat, which is due to applying correspondence analysis. In case multiple ranks are listed, the first has the strongest and the last has the weakest influence on the respective threat. Additionally, the proportion of teachers who experienced digital threats first-hand is shown.

Table 1

Teachers' ranking as discussed by Taupe *et al.* (2025) and first-hand experience in regards of digital threats by Taupe *et al.* (2023).

Threat	Ranks	Experience	Threat	Ranks	Experience
Inappropriate Content	1	30.93 %	Social Media Addiction	1	43.93 %
Illegal Content	2	17.37 %	Gaming Addiction	2	40.54 %
Purchase Illegal Substances	3	7.91 %	Shopping Addiction	3	7.91 %
Information Overload	1	47.32 %	Cyber Mobbing	1	36.16 %
Fake Information	2	38.42 %	Cyber Stalking	2	15.82 %
Computer/Data Damage	6	18.50 %	Violence/Crime Incitement	4, 5, 3	11.44 %
Reputation	5, 6	16.95 %	Injury Trivialization	6	10.17 %
Data Breach	4, 5	15.68 %	Contact Strangers	4, 5, 3	8.62 %
Personal Privacy	4	8.19 %	Happy Slapping	4, 5, 6	6.78 %

5. Results

When referring to the perspective of different generations, we apply the generation definition of Klein (2020): Generation X: 1965–1979; Generation Y: 1980–1995. To keep the statistical power of the analysis as high as possible, the central limit theorem recommends using 30 or more samples. With this in mind, only items with at least 30 participants have been included in the tables – this applies to gender, generation and region breakdowns. Of the total of 278 participants, 80.21 % were female, 18.71 % were male and 1.08% did not specify their gender.

Fig. 1 shows a box plot that indicates the median age at which children and teenagers have the ability to use the Internet without restrictions. This means parents no longer need to monitor or supervise their children in regards of using the Internet safely. The cross indicates that parents specify a mean value of 15.73 years (±2.95 years; median 16 years).

Fig. 2 shows the proportion of parents who monitor how their children use the Internet. The majority of 71.58 % indicate to monitor their children in some way. Parents make use of different measures (from left to right in the figure): using an app on the smartphone, other measures or by checking how their children use different media (e. g., browsing history). Parents who do not monitor their children also specify different reasons (from left to right in the figure): children are grown up, parents do not know how, other reasons or parents see no need.

We asked parents to rank digital threats according to how often young people may be exposed to them. Overall, the rankings reveal distinct category-specific patterns of association between threats and perceived exposure frequency. Fig. 3 illustrates the relationship between ranks (red arrows) and threats (blue dots) within each category, based on the first two dimensions from the correspondence analysis, which together explain most of the variance. The categories “Content Harmful to Young People” and “Online Addiction” are fully explained by two dimensions, with clear alignment be-

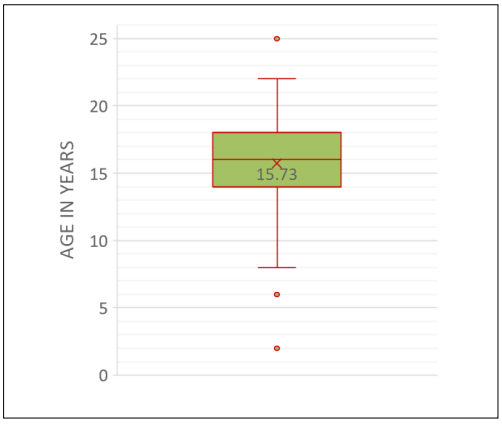

Fig. 1. Ability of young people to use the Internet without restrictions from the perspective of parents.

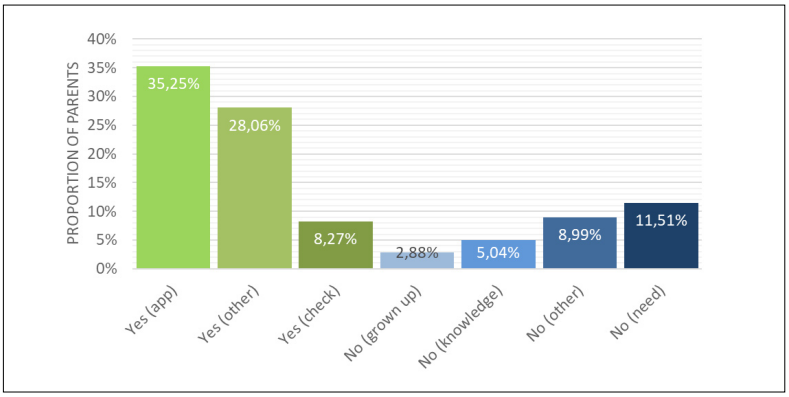

Fig. 2. Do you control how your children use the Internet?

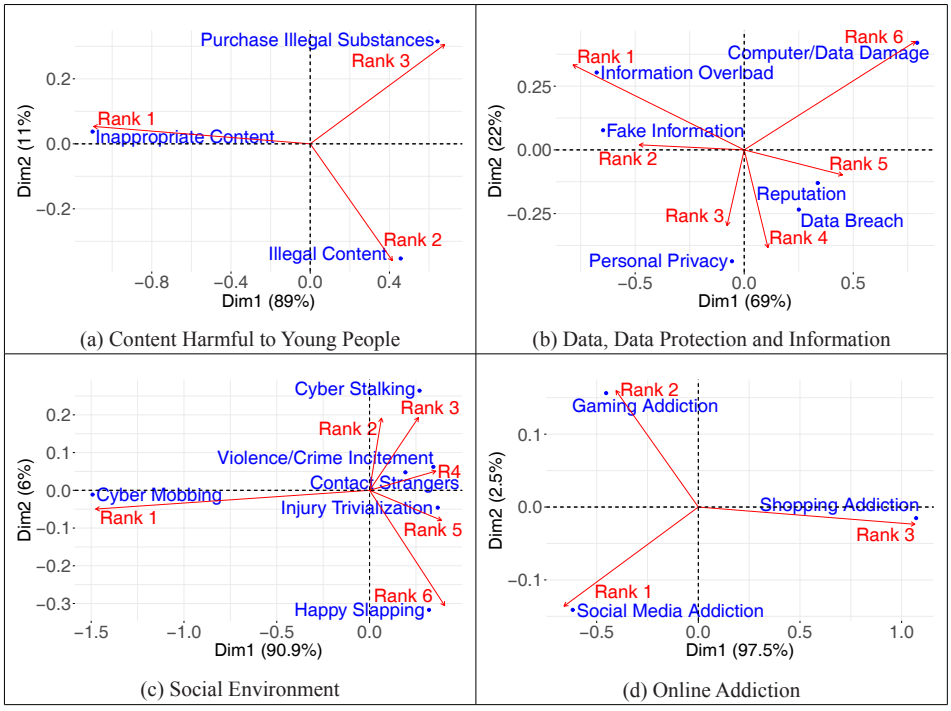

Fig. 3. Individual ranking of digital threats within their respective category.

tween specific threats and the ranks that most influence them. The categories "Social Environment" and "Data, Data Protection and Information" are described by five dimensions each, though the first two capture the main variance of the data. The length of an arrow indicates the relative strength of a rank's influence; the closer a threat lies to an arrow's tip, the stronger that association. For example, the digital threat *Fake Information* in Fig. 3b lies at the far end of the second-rank arrow while also moving toward

Table 2
Parents' first-hand experience on digital threats for children and teenagers

Threat	Experience	Threat	Experience
Inappropriate Content	30.22 %	Social Media Addiction	35.61 %
Illegal Content	8.27 %	Gaming Addiction	35.61 %
Purchase Illegal Substances	5.40 %	Shopping Addiction	10.07 %
Information Overload	48.56 %	Cyber Mobbing	22.30 %
Fake Information	36.69 %	Contact Strangers	8.63 %
Data Breach	19.42 %	Injury Trivialization	6.12 %
Personal Privacy	15.11 %	Happy Slapping	4.68 %
Computer/Data Damage	11.87 %	Violence/Crime Incitement	3.96 %
Reputation	8.27 %	Cyber Stalking	3.96 %

the first rank, indicating primary influence from rank 2 and secondary influence from rank 1. These patterns show that parents associate certain threats strongly with specific ranks, while others display more complex, multi-rank influences.

Table 2 shows the share of all participating parents who have already experienced or witnessed at least one case first-hand where a child or teenager has been involved in an incident regarding the aforementioned digital threats.

Table 3 shows the overall proportion of parents in regards of their experience, from different perspectives like gender, generation and region. This includes parents reporting indirect experience as well as parents who report to have no experience at all. Indirect experience means they have not experienced a case first-hand but know someone who has.

6. Discussion

In this study, we asked parents which they consider the proper age of young people to use the Internet safely without restrictions. Fig. 1 shows that 50 % of all responses are between 14 and 18 years with a mean of 15.73 years (±2.95 years). Parents report that they allow children or teenagers to access the Internet without restrictions at an average age of 15.36 years (±2.08 years), while 50 % of parents' answers are between 14 and 16 years. This implies that, on average, parents allow their children to use the Internet without restrictions around the age parents think their children have the proper age to do so. Regarding both questions, the median is 16 years, which is nearly equal to each respective mean value. This indicates a symmetric distribution of the data with few outliers, reducing its bias. One interesting aspect is that in the previous study, teachers estimated that young people access the Internet without restrictions at an average age of 9.04 years (±2.44 years). Of all answers, 50 % were between 7 and 10 years. The different views of teachers and parents may be due to their different perspectives, children's digital competencies, safety concerns, and maturity and judgment considerations. Teachers may believe that young people can use the Internet at an earlier age

Table 3
Parents' experience on digital threats for children and teenagers from different perspectives like gender, generation and region

	First-Hand Experience	Indirect Experience	No known Incident
Overall	70.50 %	14.03 %	15.47 %
Female	71.75 %	13.00 %	15.15 %
Male	63.46 %	19.23 %	17.31 %
Generation X	72.22 %	12.70 %	15.08 %
Generation Y	69.86 %	15.07 %	15.07 %
Tyrol	74.76 %	11.65 %	13.59 %
Carinthia	67.07 %	17.07 %	15.86 %
Vienna	58.06 %	12.90 %	29.04 %

safely, because they see children's educational use of the Internet as well as their digital competencies. On the other hand, parents may have greater security concerns and believe that maturity and judgment are crucial to using the Internet safely. This can also encourage them to monitor how their children use the Internet. Both views are valid and the ideal age for unsupervised use of the Internet may vary. In the best-case teachers and parents work together to ensure children's online safety.

Table 3 shows that 70.50 % of all participating parents have already experienced or witnessed at least one incident first-hand in relation to digital threats. Another 14 % indicate to at least know someone how has and 15 % experienced no such incident at all. Compared to the teacher study, also 71% of participating teachers stated to have had firsthand experience with at least one of these threats. These findings show that both, parents, and teachers, understand that children and teenagers are confronted with various digital threats. From the perspective of federal states, the information provided by parents differs noticeably. While indirect experience does not differ that much, values indicating firsthand experience show clear differences. Values appear to be higher in the west of Austria (e. g., Tyrol), whereas the values are lower in the south of Austria (e. g., Carinthia) and in the north (e. g., Vienna). Possible reasons can be the quality of digital educational resources, less robust digital infrastructure and limited access to reliable Internet in rural areas. Additionally, it is important that both parents and children in these areas are informed about possible digital threats and how to safely use the Internet. Apart from the geographical location, this could also indicate a relation to the proportion of people living in urban areas. In this case, this would implicate that values are higher in rural areas compared to urban areas. This could mean that in urban areas less incidents happen, or that parents are less sensible in regards of noticing.

Table 2 shows values in regards of parents' first-hand experience with digital threats while Table 1 presents values from teachers' perspective. According to the findings of both studies, some differences can be observed.

Fig. 3 shows the individual ranking of threats from parents' point of view, utilizing correspondence analysis instead of relative frequencies. The reason is to better

understand the association between threats and ranks. The goal of this study is to compare the results with the teacher study and prioritize threats within their respective categories. Fig. 3a shows how parents ranked threats in the category "Content Harmful to Young People". The threats *Inappropriate Content*, *Illegal Content* and *Purchase Illegal Substances* are clearly associated with ranks one to three, in that order. Comparing these results to the findings of the teacher study yields the same result. Threats of category "Online Addiction" emit a similar image, as shown in Fig. 3d. Threats *Social Media Addiction*, *Gaming Addiction* as well as *Shopping Addiction* have been ranked from rank one to three. Threats of this category show the same pattern as in the teacher study. Fig. 3b emerges a more varying result for category "Data, Data Protection and Information". The threat *Information Overload* was ranked first very clearly, followed by *Fake Information* ranked second. *Personal Privacy* has a strong association to the third rank, but is also slightly influenced by the fourth rank. Similar can be observed for threats *Data Breach* and *Reputation*. Both are associated with ranks four and five, whereas *Data Breach* is stronger associated to rank four and *Reputation* is stronger associated to rank five. The threat *Computer/Data Damage* is associated to rank six. Comparing this result to the findings of the teacher study yields a very similar pattern. Fig. 3c shows how threats of the category "Social Environment" have been ranked by parents. Threat *Cyber Mobbing* was ranked first very clearly. There seems to be no clear association between a threat and rank two. *Cyber Stalking* shows an association to rank three with a slight influence of rank two. Followed by threat *Contact Strangers*, which shows an association to rank four, but is obviously influenced by lower ranks. The threat *Violence/Crime Incitement* is strongly associated with rank four, followed by *Injury Trivialization* with rank five. Rank six is mostly associated with the threat *Happy Slapping*. When also considering the result of the teacher study, associations are quite similar. Threats *Contact Strangers* and *Violence/Crime Incitement* are ranked very similar. While *Happy Slapping* was ranked fourth by teachers, showing a slight association to rank six as well, this threat was ranked sixth by parents. Teachers associated *Injury Trivialization* mostly with rank six, while parents associated it with rank five.

A final ranking of digital threats in the field of digital safety can be defined as shown in the following tables. Each table shows the final ranking of digital threats within their respective category. To determine the final rank of a digital threat, teachers' (see Table 1) and parents' first-hand experience (see Table 3) is used as a primary indicator. In case the relative rank in regards of first-hand experience differs, the individual ranking is used as an additional weight – which has been done by both groups. The individual ranking is the result of the correspondence analysis. Parents' individual rankings are taken from Fig. 3. The following tables also contain the ranks of teachers' individual rankings described by Taupe *et al.* (2025) and teachers' first-hand experience described by Taupe *et al.* (2023) -both presented in Table 1. Note that a threat may be influenced by more than one rank. When multiple ranks are specified for one threat, the first one indicates the rank with the strongest influence while the last one with the weakest.

Table 4 shows the ranking of threats within the category "Content Harmful to Young People". All threats have been ranked equally by both, parents, and teachers. Moreover,

Table 4

Ranking of digital threats within category "Content Harmful to Young People"
(Teacher data from Taupe *et al.* (2025, 2023))

Final Rank	Threat	Teachers'		Parents'	
		Experience	Ranks	Experience	Ranks
1	Inappropriate Content	30.93 %	1	30.22 %	1
2	Illegal Content	17.37 %	2	8.27 %	2
3	Purchase Illegal Substances	7.91 %	3	5.40 %	3

their personal first-hand experience shows the same pattern as well. Especially the threat *Inappropriate Content* seems to be a common issue. Parents as well as teachers indicate to have had plenty of experiences with this threat. When defining corresponding competencies in the future, this threat should be brought into focus. Parents and teachers have influence at this point also.

Threats assigned to category "Data, Data Protection and Information" were ranked as shown in Table 5. While threats on rank one and two are clearly ranked, the remaining show some variation. The first-hand experience of parents and teachers has been used as the main weight. Considering this, the remaining ranks can be well assigned to the respective threats. From the perspective of parents' and teachers' first-hand experience, *Personal Privacy*, *Data Breach*, *Reputation*, and *Computer/Data Damage* are swapped. When considering both, parents' and teachers' first-hand experience and using the individual ranking as an additional weight, yields the final ranks shown; ranks are very close to each other for these threats. Within this category, the threats *Information Overload* and *Fake Information* stand out. Sensitivity to threats in terms of the amount of information as well as its quality appears to be high among parents and teachers. The results show that children and teenagers are already exposed to these threats. Moreover, these threats can have a negative impact on their development and formation of opinion. For this reason, it is essential to protect young people by teaching them how to deal with information and false information appropriately, as early as possible.

Table 5

Ranking of digital threats within category "Data, Data Protection and Information"
(Teacher data from Taupe *et al.* (2025, 2023))

Final Rank	Threat	Teachers'		Parents'	
		Experience	Ranks	Experience	Ranks
1	Information Overload	47.32 %	1	48.56 %	1
2	Fake Information	38.42 %	2	36.69 %	2, 1
3	Data Breach	15.68 %	4, 5	19.42 %	4, 5
4	Computer/Data Damage	18.50 %	6	11.87 %	6
5	Personal Privacy	8.19 %	4	15.11 %	3, 4
6	Reputation	16.95 %	5, 6	8.27 %	5, 4

Table 6
Ranking of digital threats within category "Social Environment"
(Teacher data from Taupe *et al.* (2025, 2023))

Final Rank	Threat	Teachers'		Parents'	
		Experience	Ranks	Experience	Ranks
1	Cyber Mobbing	36.16 %	1	22.30 %	1
2	Cyber Stalking	15.82 %	2	3.96 %	3, 2
3	Contact Strangers	8.62 %	4, 5, 3	8.63 %	4, 3
4	Violence/Crime Incitement	11.44 %	4, 5, 3	3.96 %	4
5	Injury Trivialization	10.17 %	6	6.12 %	5
6	Happy Slapping	6.78 %	4, 5, 6	4.68 %	6

Table 6 shows the ranking of threats in category "Social Environment". Also here, basic ranking decision was made based on parents' and teachers' first-hand experience. Rank one is very clear, followed by *Cyber Stalking* assigned to rank two. In this case, the threat was strongly associated to rank two in the teacher study and between rank three and two in the study with parents. Teachers seem to experience or witness this threat more often than parents do. The same proportion of parents and teachers reported first-hand experience in regards of *Contact Strangers* – and is slightly higher than with others. Also, it shows an association to rank four in both studies with a noticeable influence of other ranks. For these reasons, this threat was ranked third, followed by *Violence/ Crime Incitement* on rank four, which shows a strong association to rank four in both studies. *Injury Trivialization* was assigned to rank five. This threat shows a strong association to rank five in the study with parents, while it is strongly associated with rank six in the teachers study. The threat *Happy Slapping* shows a strong association to rank six in the parent study, while it shows an association to rank four with a slight influence of rank six in the teacher study. Since only a very small proportion of teachers and parents stated to have had first-hand experience in addition, this threat was assigned to rank six. Particularly the threat *Cyber Mobbing* is often documented in the media and other publications. It is interesting that teachers seem to be more sensitive to such incidents than parents. One reason for this could be that teachers are better able to perceive the interactions of children at school than parents at home. In addition to its frequent occurrence, *Cyber Mobbing* poses a serious threat, particularly because of its potential impact on young people.

Last, the ranking of threats in category "Online Addiction", listed in Table 7, was straight-forward. Having a look at the first-hand experience shows that experience with *Social Media Addiction* and *Gaming Addiction* within both groups seems to be quite similar. Both, teachers and parents, associated threats with the same individual ranks. The threats in this category clearly show the different perspectives of parents and teachers in regards of children and teenagers. Concerning the overuse of social media and games, parents report fewer incidents. A possible reason could be that parents have a less drastic view of how young people use these services. When it comes to online shopping, parents may have better insight than teachers and therefore report more incidents than

Table 7
Ranking of digital threats within category "Online Addiction"
(Teacher data from Taupe *et al.* (2025, 2023))

Final Rank	Threat	Teachers'		Parents'	
		Experience	Ranks	Experience	Ranks
1	Social Media Addiction	43.93 %	1	35.61 %	1
2	Gaming Addiction	40.54 %	2	35.61 %	2
3	Shopping Addiction	7.91 %	3	10.07 %	3

teachers. Parents and teachers are particularly concerned about the use of social media and games. There is obviously a need for improvement when it comes to training for children and teenagers using such services.

The tables above show how digital threats are prioritized within their respective categories – primarily based on first-hand experience and individual ranking by teachers and parents as an additional weight. This prioritization of digital threats indicates which digital threats generally require more attention than others – with possible influence on future competency development in the field of digital safety.

7. Recommendation

Education is a vital factor in addressing digital threats for young people. Based on the findings along, it is advisable to develop competencies especially in the following areas: *Inappropriate Content, Information Overload, Cyber Mobbing and Social Media Addiction*. These areas align closely with the "Privacy, safety and security" and "Responsibility and empowerment" core topics in the Informatics Reference Framework for School (IRFS) by Caspersen *et al.* (2022), as well as with the CSTA K-12 Computer Science Standards' cybersecurity and impacts of computing strands by K-12 Computer Science Framework Steering Committee (2016)

According to Klieme *et al.* (2003), competency models describe expected learning outcomes and ways of acquiring knowledge. They serve as a basis for operationalizing educational goals and enable empirical testing of educational systems by applying testing procedures. Competency models impart between abstract educational goals and concrete tasks. They support the design of testing procedures and provide guidance for practice-oriented lesson planning – which is based on the learning processes and learning outcomes of pupils. The purpose of competency models is to describe and evaluate educational standards. Consequently, competency models follow two purposes: required competencies and levels to measure the development of pupils.

Competency models are now being created as part of a project at the University of Klagenfurt in Austria. The process is complex, and criteria such as meaningfulness, viability, etc., must also be considered when selecting the competencies. Therefore, the threats that have now been ranked are an excellent starting point for these models. Examples of competencies (formatted in italics) for the most relevant threats are listed

below. For transparency and ease of adoption, each competency below can be mapped to at least one IRFS core topic by Caspersen *et al.* (2022), one element from the European Survey's consensus areas by Nardelli *et al.* (2025), and a corresponding K-12 standard by K-12 Computer Science Framework Steering Committee (2016), providing educators and policymakers with a direct alignment pathway.

Inappropriate Content:
These competencies address IRFS core topics "Privacy, safety and security" and "Responsibility and empowerment" by Caspersen *et al.* (2022), reflect findings from the European Survey on digital safety requirements by Nardelli *et al.* (2025), and relate to K-12 standards 1B-NI-05, 1B-IC-18 and 3A-IC-24 by K-12 Computer Science Framework Steering Committee (2016).

- *Pupils are able to identify age-appropriate and inappropriate digital content and understand why certain content may not be suitable for younger audiences:* Pupils could analyze media samples (e. g., news articles, videos, or games) with varying degrees of appropriateness. They discuss why certain content may be appropriate or not – for their age group. Teachers can discuss on media ratings, exploring how they help guide safe content consumption.
- *Pupils are able to make informed choices about the content they consume online, distinguishing between trustworthy and potentially harmful sources:* Pupils practice to differ reliable websites and sources from untrustworthy ones. This can be achieved by examining fake news or clickbait headlines. They can create a checklist for assessing sources' credibility, developing habits for more sensible content selection.
- *Pupils are able to critically assess digital content to determine if it matches their values, developmental stage, or personal well-being:* Teachers may guide pupils through scenarios where they assess specific types of content (e. g., violent, sensationalized, or age-inappropriate material) – to decide if it is suitable for them. This activity can include role-playing situations where pupils face challenging content and need to decide whether it is suitable or not.

Information Overload:
Linked to IRFS "Data and information" and "Human-computer interaction" by Caspersen *et al.* (2022), incorporates European Survey emphasis on critical evaluation of online resources by Nardelli *et al.* (2025), and maps to K-12 standards 1B-IC-18, 1B-IC-19, 2-IC23 and 3A-IC-24 by K-12 Computer Science Framework Steering Committee (2016).

- *Pupils are able to recognize that excessive notifications can lead to distractions and affect their focus:* Teachers could demonstrate the impact of frequent notifications by allowing pupils to keep their devices on during a specific activity – followed by a discussion on how this affected their productivity. This raises awareness about the disruptive nature of notifications.
- *Pupils are able to assess notifications critically and decide whether immediate response is necessary:* A role-play activity where pupils receive different types of notifications (e. g., urgent, non-urgent, promotional) could be suitable. Then they

have to decide which notifications require immediate attention and which not. This activity allows pupils to practice prioritizing notifications.

- *Pupils are able to configure apps and devices to suppress unwanted notifications:* Teachers may lead a tutorial on configuring notification settings for commonly used apps – showing pupils how to silence non-essential alerts. Pupils then adjust their own devices to prioritize notifications from educational apps or essential contacts, improving self-management skills.

Cyber Mobbing:
Corresponds to IRFS "Responsibility and empowerment" and "Human-computer interaction" by Caspersen *et al.* (2022), integrates European Survey recommendations on interpersonal digital ethics Nardelli *et al.* (2025), and aligns with K-12 standards 1A-IC-17, 1B-IC-18 and 3A-IC-24 K-12 Computer Science Framework Steering Committee (2016).

- *Pupils are able to communicate online in a safe, responsible, and respectful manner:* Teachers could offer a workshop on digital etiquette, where pupils role-play online scenarios that can lead to misunderstandings. They practice respectful responses, and teachers guide discussions on how tone and language can impact online interactions. This helps them develop empathy, foster positive interactions and avoid unintentional conflicts.
- *Pupils are able to use digital self-defense techniques to protect themselves:* Pupils receive hands-on training in using platform-specific blocking and reporting functionalities. Teachers create a checklist for steps to take if pupils experience or witness cyber mobbing. This empowers pupils to take immediate protective actions online.
- *Pupils are able to empathize with the impact of cyber mobbing on victims and understand the potential consequences for perpetrators:* In a reflective activity, pupils read or watch stories from individuals who have experienced cyber mobbing. Afterwards they discuss how such incidents affected the victims. This fosters empathy and improves their understanding of possible consequences online actions can have on others.

Social Media Addiction:
Aligns with IRFS "Responsibility and empowerment" and "Privacy, safety and security" by Caspersen *et al.* (2022), reflects European Survey observations on student well-being in digital contexts by Nardelli *et al.* (2025), and links to K-12 standards 1A-IC-17 and 1B-IC-18 by K-12 Computer Science Framework Steering Committee (2016).

- *Pupils are able to strengthen their self-esteem by recognizing their personal strengths and achievements:* Pupils create a "Strengths Journal" where they regularly record things they have accomplished or feel proud of. Teachers can guide group discussions where pupils share positive experiences offline, helping them build self-esteem through real-world achievements instead of social media likes or followers – reducing their need to seek validation online.
- *Pupils are able to manage social conflicts with suitable strategies:* Pupils practice conflict-resolution techniques, such as active listening in group activities. Teach-

ers could foster discussions about how positively resolving real-world conflicts can lead to stronger friendships. As a side effect this also reduces the urge to seek validation or comfort on social media.

- *Pupils are able to choose appropriate social media platforms and use safety features:* Teachers may introduce pupils to privacy settings on popular platforms, showing how to use them effectively. Pupils practice adjusting settings to control their online presence. Followed by discussions with pupils about how using social media safely can contribute to a more positive digital experience.

The recommended competencies are not limited to informatics-related competencies; rather, they include technical, social, and emotional dimensions which can be addressed across various educational areas. While certain aspects may overlap with existing informatics curricula, the broader scope of these competencies suggests that their teaching need not be limited to computer science classes. This enables more flexible integration into diverse learning environments. Moreover, as outlined above, these competencies can be mapped to established frameworks such as the Informatics Reference Framework for School by Caspersen *et al.* (2022), the European Survey consensus areas by Nardelli *et al.* (2025), and the K-12 Computer Science Standards by K-12 Computer Science Framework Steering Committee (2016). However, the competencies developed in this work are defined in a more explicit and detailed manner, providing teachers with clearer guidance for targeted and effective instruction.

8. Validity and Limitations

With reference to internal validity, the following may have an impact on the findings. When parents share their experience through the survey, they can be influenced by societal expectations, or they may overrate or underrate specific digital threats. Since individual ranking and relative ranks of threats regarding first-hand experience match on the whole, this is not expected to be an issue here. Apart from that, negative first-hand or indirect experience with specific threats may influence parents' ranking of those in contrast to such with no experience. Parents may have difficulty remembering all incidents or events that occurred in the past. While the gender distribution among parents may not exactly match the total population in Austria, this does not necessarily have an impact on representativeness. Parents bring diverse experiences that enrich societal understanding. The gender distribution among parents can change over time, reflecting societal shifts and providing valuable insights. Including all parents ensures their experiences are represented. Therefore, the differing gender distribution offers a unique, equally important viewpoint, rather than negatively impacting representativeness. From a gender perspective, there is a difference on votes for first-hand and indirect experience with threats. When experience with threats is seen as a whole, values show minor differences. This possibly indicates that female parents are more sensible in relation to this topic, or they spend more time with children and teenagers on the whole. This circumstance may cause a small error, meaning the actual number of incidents to be slightly different in reality. Participation rate varied across federal states, which is

not expected to be a major source of error, but should be taken into account in further considerations. Differences in regional response rates and gender representation may influence the extent to which the findings can be generalized to the wider population. For example, regions with lower participation might contribute less to the aggregate trends, potentially under-representing local priorities. Nevertheless, the consistency of patterns observed across the larger subgroups provides confidence in the robustness of the prioritization results.

Regarding external validity, parents participated on a random basis. Parents' associations have been contacted and asked to distribute the invitation to the study. Since parents participated voluntarily, there is a chance that parents with an opinion or experience about the topic digital safety were more likely to participate in the survey, than parents with no prior experience or interest in this area. It was not possible to control how the invitation to the study was shared with other people by parents who initially received an invitation. Parents might have distributed the link to people they know. One indicator that this has happened is, that seven participants reported to not have children at all. The data of these participants have been excluded from the original 285 participants and the analysis. Anyhow, the chance that the survey was distributed by some participants is not expected to be an issue. The online questionnaire measurement instrument was designed to mitigate systematic errors or biases. For example, all questions required active response, without providing default values or suggestions. In regards of the ranking tasks, the initial positioning of items to rank was randomized for each participant. Parents could decide on their own when to participate. The setting did not pressure parents to participate and no thank-you gift was promised.

While the sample is limited to the participating parents and teachers, the combined datasets are sufficiently large and diverse to support the prioritization patterns identified in this study. The overall analysis includes responses from 278 parents and 708 teachers, providing complementary perspectives from two key groups. This integrated evidence base underpins the robustness of our conclusions, even though, as with any survey, results may not capture every possible viewpoint.

Another aspect of this study is that the perspective of pupils was not included. This decision was made because of practical and ethical constraints, including approval restrictions. The sensitive nature of some topics was another reason, which in certain cases include child protection regulations. While this study focuses on the perspectives of teachers and parents, we acknowledge that including the perspective of pupils could potentially lead to some variation in the prioritization of certain digital threats. However, given the close involvement of teachers and parents in the digital lives of young people, we do not expect major divergences. Including the perspective of pupils in future studies would add further depth – where ethically and practically feasible.

The proposed competencies were derived from the empirical findings of this study. While they were not formally reviewed or piloted with educators within the scope of this work, their alignment with established research supports their conceptual soundness. Future research should incorporate systematic expert feedback and small-scale implementation to further refine and validate their applicability in practice.

The study was conducted in Austria and provides valuable insights, which are likely applicable to countries with a similar cultural background. To our knowledge, this is the first study of this kind and the results are very useful, even taking these limitations into account. We hope that this study will trigger further research in this area, as it has not perceived the necessary attention.

9. Conclusion

Various publications mention threats in the digital realm, which have been gathered and categorized – however, up to now there was no ranking available. In a previous study, conducted in early 2023, teachers in Austria have been surveyed in order to find out what digital threats in the field of digital safety are considered more relevant to children and teenagers than others. The current study, which surveyed parents in Austria, unveils additional insights. Subsequent to existing publications, reporting on parents' digital competencies and awareness by Łukasz Tomczyk (Tomczyk, 2018), Arifin *et al.* (2019), and Łukasz Tomczyk and Potyrała (Tomczyk and Potyrała, 2021), the situation has already improved: According to the present findings, parents are aware of various threats in the digital realm. Parents indicate to care about how children and teenagers use the Internet. The age at which children and teenagers are able to use the Internet without restrictions, from parents' point of view, may be reasonable, provided that the necessary competencies are appropriately taught.

This research contributes to the scientific community by identifying and prioritizing the most urgent digital threats in the educational context – from the perspectives of teachers and parents. It was possible to develop a comprehensive prioritization of threats in the field of digital safety by examining the findings of this study as well as those of the already existing teacher study. Primarily the first-hand experience of parents and teachers has been considered – which corresponded well in most cases. In some cases, individual ranking of parents and teachers has been used as an additional weight to provide a comprehensible ranking. Threats within the categories *Content Harmful to Young People* and *Online Addiction* exhibit the same pattern in regards of first-hand experience for all threats in the teacher and the parent study. Threats in the category *Data, Data Protection and Information* show different first-hand experience for teachers and parents – except for threats ranked first and second. The same was observed for the category *Social Environment*, where only the first ranked threat shows similar first-hand experience for teachers and parents. This required deeper considerations for prioritizing threats within these categories. This may indicate that both, parents and teachers, not just ranked the threats based on their personal experience, but also took other aspects into account, which is considered positively.

Digital media and devices are used globally. Although this study was carried out in Austria, the identified digital threats and corresponding competencies are not bound to the national context. Given the global nature of digital technologies, online risks, and youth media use, we expect these findings to be largely transferable to educational contexts in other countries. Nonetheless, future research in different cultural and edu-

cational settings would allow for examining potential context-specific variations and strengthen the generalization of the results. We hope that our study will trigger similar research in other countries to understand threats from a broader perspective and improve digital education in all countries. Based on the prioritization, competencies can be defined to improve the digital safety of young people in the future. This includes all of the aforementioned digital threats, whereas the prioritization can be used as an indicator of how important it is to develop further competencies for a specific digital threat. Anyhow, our findings show there is a major need for developing suitable competencies for the following digital threats: *Inappropriate Content, Information Overload, Fake Information, Cyber Mobbing, Social Media Addiction* and *Gaming Addiction*. A next step may be a qualitative study, interviewing teachers and parents. A complementary study with pupils could be conducted in the context of digital threats as well. By considering other data, like at which age different threats are relevant for children and teenagers, can make a positive contribution to the definition of appropriate competencies and to provide a safer environment for our children in the future.

References

Aigner, R., Kofler, M., Zingsheim, A., Gebeshuber, K., Kania, S., Widl, M., Kloep, P., Hackner, T., Neugebauer, F. (2020). *Hacking & Security: das umfassende Handbuch* (2nd ed.). Rheinwerk Verlag, Bonn, Germany. 9783836271912.

Arifin, N.A., Mokhtar, U.A., Hood, Z., Tiun, S., Jambari, D.I. (2019). Parental Awareness on Cyber Threats Using Social Media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2), 485–498. https://doi.org/10.17576/JKMJC-2019-3502-29

Bundesministerium für Bildung, Wissenschaft und Forschung (2023a). Gesamte Rechtsvorschrift für Lehrpläneder Mittelschulen. StF: BGBl. II Nr. 185/2012. Änderung BGBl. II Nr. 1/2023, Vienna, Austria.

Bundesministerium für Bildung, Wissenschaft und Forschung (2023b). Gesamte Rechtsvorschrift für Lehrpläne – allgemeinbildende höhere Schulen. StF: BGBl. Nr. 88/1985. Änderung BGBl. II Nr. 1/2023, Vienna, Austria.

Bundesministerium für Digitalisierung und Wirtschaftsstandort (2021). Digitales Kompetenzmodell für Österreich: DigComp 2.2 AT. Accessed: 2024-09-05. https://www.bmaw.gv.at/dam/jcr:54bbe103-7164-494e-bb30-cd152d9e9b33/DigComp2.2_V33-barrierefrei.pdf

Bundesministerium für Inneres, Bundeskriminalamt (2023). Polizeiliche Kriminalstatistik 2022: Die Entwicklung der Kriminalität in Österreich. Accessed: 2024-09-29. https://bundeskriminalamt.at/501/files/2023/PKS_Broschuere_2022.pdf

Carretero, S., Vuorikari, R., Punie, Y. (2017). *DigComp 2.1 – The digital competence framework for citizens with eight proficiency levels and examples of use*. Publications Office of the European Union. 978-92-79-74173-9. https://doi.org/doi/10.2760/38842

Caspersen, M.E., Diethelm, I., Gal-Ezer, J., McGettrick, A., Nardelli, E., Passey, D., Rovan, B., Webb, M. (2022). *Informatics Reference Framework for School*. Informatics for All. https://doi.org/10. 1145/3592625.

Council for Crime Prevention in Schleswig-Holstein (2007). Happy Slapping und mehr -Brutale, menschenverachtende oder beleidigende Bilder auf Handys. (nicht mehr verfügbar). https://www.datenschutzzentrum.de/schule/happy-slapping.pdf

Cypra, O. (2005). *Warum spielen Menschen in virtuellen Welten? Eine empirische Untersuchung zu Online-Rollenspielen und ihren Nutzern*. Diplomarbeit der Johannes Gutenberg Universität Mainz: Institut für Soziologie.

Drechsler, D., Haag, D., Hertwig, O., Rohrer, A., Schmid, M.D. (2019). *Schutz vor Social Engineering: Angriffspunkte und Abwehrmöglichkeiten in digitalwirtschaftlichen Ökosystemen*. Erich Schmidt Verlag, Berlin, Germany. 9783503188598.

Eichenberg, C., Auersperg, F. (2018). *Chancen und Risiken digitaler Medien für Kinder und Jugendliche: ein*

Ratgeber für Eltern und Pädagogen (1st ed.). Hogrefe, Göttingen, Germany. 9783840926471.

Eichenberg, C., Kühne, S. (2014). *Einführung Onlineberatung und -therapie*. Ernst Reinhardt, München. 9783825241315.

Europol (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Publications Office of the European Union, Luxembourg. 978-92-95236-34-9. https://doi.org/10.2813/442713

Gasser, U., Cortesi, S., Gerlach, J. (2012). *Kinder und Jugendliche im Internet: Risiken und Interventionsmöglichkeiten* (1st ed.). hep, Bern, Switzerland. 9783039059072.

Glaser, S., Günter, T., Höhler, L., Schindler, F., Wittstadt, H. (2010). Jugenschutz im Internet. Ergebnisse der Recherchen und Kontrollen. Bericht 2010, Mainz. (nicht mehr verfügbar). http://www.jugendschutz.net/fileadmin/download/pdf/bericht2010.pdf

K-12 Computer Science Framework Steering Committee (2016). K-12 Computer Science Framework. Technical report, New York, NY, USA. 9781450352789.

Klein, C. (2020). Jede Generation hat eigene Werte – Generation Z. *physiopraxis*, 18(1), 58–60. https://doi.org/10.1055/a-0975-1796

Klieme, E., Avenarius, H., Blum, W., Döbrich, P., Gruber, H., Prenzel, M., Reiss, K., Riquarts, K., Rost, J., Tenorth, H.-E., Vollmer, H.J. (2003). *Zur Entwicklung nationaler Bildungsstandards. Eine Expertise*. 1. BMBF, Bonn, Berlin. https://doi.org/10.25656/01:20901

Koerrenz, R., Diergarten, P. (2022). *Fake News und andere Realitäten -'Was ist Wahrheit?'*. Vandenhoeck & Ruprecht. 9783647703237.

Külling, C., Waller, G., Suter, L., Willemse, I., Bernath, J., Skirgaila, P., Streule, P., Süss, D. (2022). *JAMES -Jugend, Aktivitäten, Medien -Erhebung Schweiz*. Zürcher Hochschule für Angewandte Wissenschaften, Zürich, Schweiz.

Little, T.D. (2013). *The Oxford Handbook of Quantitative Methods, Vol. 2: Statistical Analysis* (1st ed.). Oxford University Press. 9780199934898.

Nardelli, E., Futschek, G., Gal-Ezer, J., Webb, M. (2025). *A European survey on requirements for the informatics school curriculum and informatics school teachers' education*. Informatics for All.

O'Keeffe, G.S., Clarke-Pearson, K., Council on Communications and Media (2011). The Impact of Social Media on Children, Adolescents, and Families. *Pediatrics*, 127(4), 800–804. https://doi.org/10.1542/peds.2011-0054

Palfrey, J., Gasser, U. (2008). *Generation Internet: Die Digital Natives: Wie sie leben -Was sie denken -Wie sie arbeiten* (1st ed.). Hanser, München. 978-3446414846.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Taupe, J., Knapp, V., Bollin, A. (2023). Teachers' Experience Regarding Digital Threats for Children and Teenagers. In: *16th International Conference on Informatics in Schools, ISSEP 2023, Local Proceedings*. Zenodo, Lausanne, Switzerland, pp. 237–240. https://doi.org/10.5281/zenodo.8432020

Taupe, J., Knapp, V., Bollin, A. (2025). Teachers' Insight: Digital Threats that Imperil Children and Teenagers. In: *4th IFIP TC3 Open Conference on Computers in Education (OCCE 2024)*. IFIP Advances in Information and Communication Technology. Springer Cham, Bournemouth, United Kingdom, pp. 51–62. https://doi.org/10.1007/978-3-031-88744-4

Tintori, A., Ciancimino, G., Bombelli, I., De Rocchi, D., Cerbara, L. (2023). Children's Online Safety: Predictive Factors of Cyberbullying and Online Grooming Involvement. *Societies*, 13(2). https://doi.org/10.3390/soc13020047

Tomczyk, Ł. (2018). Digital competences of parents in the matter of electronic threats. *SHS Web Conf.*, 48(01004). https://doi.org/10.1051/shsconf/20184801004

Tomczyk, Ł., Potyrała, K. (2021). Parents' knowledge and skills about the risks of the digital world. *South African Journal of Education*, *41*(1). https://doi.org/10.15700/saje.v41n1a1833

J. Taupe holds a master's degree in Advanced Security Engineering from the University of Applied Sciences, FH Joanneum, Austria. He subsequently earned a PhD in Informatics Didactics from the University of Klagenfurt, Austria. Since 2008, he has been working as a software engineer in the private sector, combining extensive industry experience with academic research. His scholarly interests center on fostering and advancing the digital competencies of young people.

R.W. Alexandrowicz is head of the Methods Department of the Psychology Institute at the University of Klagenfurt. His major research topics are Item Response Theory, Structural Equation Modeling and Response Time Modeling.

A. Bollin completed his studies in Telematics at the Graz University of Technology, followed by a PhD in Computer Science from the Alpen-Adria-Universität Klagenfurt. He is currently the Head of the Department of Informatics Didactics at the University of Klagenfurt. His research interests include competency models in computer science education, didactics, e-learning, formal languages, gender issues in computer science education, personality-optimized education, and software engineering.

P. Schartner currently holds the position of an associate professor in the System Security Research Group at Klagenfurt University, teaching courses on cybersecurity, cryptography, and algorithms and data structures. His research interests include applied cryptography, key management, security infrastructures, and embedded security. Due to his teaching and third mission activities and his position as the DPO of Klagenfurt University, he is also interested in security awareness topics.