Hedayah
countering violent extremism

Project funded by the
EUROPEAN UNION

Passage4prevent:

The use of education
to prevent youth online radicalization

Response to Online Radicalization: Towards On-line Safety Education Policy

Marija Risteska, Metodi Hadji-Janev and Samet Shabani

CRPM Center for Research and Policy Making
... policy impact since 2004

Cyber Security, Corporate Security and Crisis Management Initiative

Skopje, 2021

Hedayah
countering violent extremism

Project funded by the
EUROPEAN UNION

This publication was produced with the project"

Passage4prevent:
The use of education
to prevent youth online radicalization

For the publisher: Center for research and policy making

Authors: Marija Risteska
Metodi Hadji-Janev
Samet Shabani

Design: Armarium Grup

Skopje, 2021

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of Center for Research and Policy Making and does not necessarily reflect the views of the European Union nor of Hedayah"

Contents

Executive Summary

Digitalization of education is an ongoing process for decades. The Covid-19 crises have accelerated its pace, putting the safety on the internet in education as a priority reform topic for every country. North Macedonia faces both online radicalization as a risk coupled with the absence of a policy framework that tackles issues related to internet safety at school, making the main issue of interest for this paper responding to online radicalization through education policy on online safety an absolute necessity for education policymakers.

The paper aims to inform that policy debate on the introduction of internet safety education policy. For that purpose, firstly, it presents the problem-online radicalization and the factors contributing to the problem, linking it with evidence on how to spread these factors are among high school students from Skopje, Tetovo, Gostivar, Veles, Kumanovo, and Shtip. Secondly, the paper provides a policy analysis of cybersecurity, education, and prevention from the violent-extremism policy framework and how these frameworks respond to the situation, mitigating the vulnerabilities of high school students to be exposed to factors that contribute to the online radicalization phenomena. Finally, the policy paper presents the proposed solution to encompass legislative responses, policy response on school level, building capacity and awareness of students, teachers and parents. Finally, the policy paper recommends several tools that can be adapted to the needs of educational organizations and communities to ensure proper internet safety policies that will prevent online radicalization.

Introduction

The internet, in particular social media, is being used as a channel, to not only promote and engage but also as a command structure for radicalization that can lead to violent extremism. Often this promotion glorifies violence, attracting and influencing many people, including children, and in extreme cases, radicalizing them. In addition, another trend occurs of promoting suffering that triggers empathy and personification with the cause (especially among women), which eventually may lead to adopting radical behavior to achieve certain objectives.

Having a strategy for safety on the internet in education, considering that youth spend most of their time in schools, is a priority for any country. Hence, countries with experienced foreign fighters' phenomena should prioritize efforts to set online safety standards, build capacities and continuously raise awareness.

This policy paper is intended to inform the education policy development towards online safety. It has been developed using multiple methods: (i) desk-top research, (ii) face-to-face interviewing of key stakeholders who, for the purpose of the paper, remain anonymous, and (iii) primary data findings

from the CRPM baseline assessment on the use of education to prevent youth online radicalization1.

The paper follows a policy problem-solution methodology. First, it presents the problem, online radicalization, and its scope in North Macedonia, then provides an analysis of the policy addressing this problem. At the conclusion, the paper offers recommendations on how the education policy and the school policy can be improved to resolve the problem. To that end, the recommendations include legislative changes, plan for professional development of high school workers and advocates for including online safety in the school curricula, Furthermore, the paper gives recommendations for a comprehensive e-safety response at school level.

[1] The survey was conducted from February until March 2020, in the municipalities of Kumanovo, Shtip, Veles, Tetovo, Gostivar and City of Skopje, on a representative sample of 756 students. The report is available at: http://www.crpm.org.mk/wp-content/uploads/2021/02/P4P_Research-Report-%D0%9C%D0%9A%D0%94-%D0%9F%D0%A0%D0%95%D0%92%D0%9E%D0%94-%D0%BB%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D1%80%D0%B0%D0%BD%D0%BE.pdf?fbclid=IwAR1wLdERnOQPbLhlSc3X6BEP4FumfT9fXYZvZdYCbXTiixEKAX-SBh7qL7Q

Why focus on internet safety?

About 250,000 students since March 2020 attend online education and contribute to the rising trend of internet usage by youth in the Republic of North Macedonia (hereinafter Macedonia), which according to the State Statistical Office, amount to 99.5% of the young people aged between 15 to 24 years old in 2019[2]. Adolescence is a time characterized by idealism, with a tendency towards all-or-nothing thinking. Moreover, they spend approximately 6 hours per day on the internet, mostly using social media networks and watching videos[3].

High school students are highly dependent on peers for a sense of wellbeing, needing to feel as if they are part of a group – yet also wanting to be viewed as unique, and their 'currency' is likes and ratings. CRPM's "***Passage4Prevent: use of education to prevent youth online radicalization***" baseline assessment offers additional findings for high school students in Gostivar, Kumanovo, Skopje, Shtip, Tetovo, and Veles, noting that 99% of the students have internet access in their home, out of which, 85% said that they have access always, while there are no rules on the use of the internet in 74.4% of the homes. Almost half of the students accept parental supervision (44,1%), whereas more than half (55, 9%) think parental supervision or control is unnecessary.

The schools, on the other side, have no policy for safe use of the internet and do not include in their curriculum education and awareness-raising on privacy and cybersecurity issues. These results in 26.4% of the high school students sometimes sharing their user's name and password with their friends, and 33.8% high school students using the automatic 'save option' for their accounts on the internet browsers. Hence, only 10% of the surveyed high school students feel unsafe online, and 8.5% have had bad personal experiences.

Considering that the country has experienced the process of youth radicalization, which was especially visible during the Syrian conflict,

---

[2] State Statistical Office, MAKStat Database, online accessed at: http://makstat.stat.gov.mk/PXWeb/pxweb/en/MakStat/MakStat_InfOpstestvo_DomakinstvaPoedinci/325_InfOpst_Mk_050_Int3mLica_mk.px/table/tableViewLayout2/?rxid=01468531-a0c4-42ac-8159-fb98946968f2

[3] Youth Study North Macedonia 2018/2019, Friedrich Ebert Stiftung, pg. 16, online accessed at: http://library.fes.de/pdf-files/id-moe/15266.pdf

through “foreign terrorist fighters” phenomena (over 140 fighters), mainly from Skopje (Chair, Gazi Baba), Kumanovo, Lipkovo, Tetovo; and the ongoing process of their return in the country (83 have been repatriated and trialled under the Criminal code article 322a which has been introduced in 2014, as well as other 23 persons who have not been trialled as their return happened before the changes of the law and criminalization of the act to mobilize and serve in the foreign army). The remaining foreign fighters and their families are expected to be repatriated soon. For this reason, the Government has adopted a National Action Plan for Rehabilitation, Resocialization, and Reintegration of foreign fighters and their families. In addition, the interethnic relations in the country between the communities continue to be tense, especially in parts of the country, where the extremist groups are still present and active, which are disposed to use the violence for achieving their political goals. Some of these processes are happening online, as Moonshot CVE efforts[4] to respond to an emerging trend of online radicalization have encompassed a comprehensive online and offline campaign for both countering the messaging of international terrorist and violent extremist organizations in the country while acting to prevent the risks of extremist messaging through activities targeting drivers that contribute to these risks, particularly among young people[5]. However, a more comprehensive strategy and policy for monitoring, controlling, preventing and promoting of safe online practices are needed.

[4] For more details see https://moonshotteam.com/
[5] Countering Violent Extremism Organizations Recruitment in Georgia, Azerbaijan and Macedonia, available online: https://www.ph-int.org/program/242/

How online radicalization works?

Increased time spent online means that children are continuously presented with moral and ethical choices as content producers and consumers (Day, 2016) and are already active decision-makers in the process. In Macedonia, while the foreign fighters were imprisoned as their activity was criminalized, there is available evidence that they are still active on the internet and that their FB pages are very popular among youth. Therefore, high school students, encounter the most risk, but they lack the skills, coping strategies and resilience to cope. If they are not trained, their vulnerabilities (with online vulnerabilities generally explained by similar factors to those that account for offline vulnerability and risk) will remain.

It is a well-accepted argument that modern technologies such as the internet and online communication applications are double-edged. These technologies provide many advantages but also introduce many risks. State and non-state actors are abusing these technologies to further their objectives, thus blurring the lines between advantages and risks that straddle the boundaries of individual safety and security (emotional/psychological, economic) through the use of cyberspace by terrorist organizations at a lower end and by national security agencies at a higher end. Hence, tools and mediums that ensure the commodity and wellbeing of our society have become threat vectors.

Building digital resilience efforts aim to strengthen the child's ability to correctly identify and interpret the impact and repercussions of the various online risks to radicalization and to develop both the technical and emotional competencies to deal with extremist propaganda and recruitment. Thus, it is required to build high school student's knowledge and awareness around online risks without focusing exclusively on particular or immediate risks. Vandoninck, d'Haenens, and Smahel (2014) found that when children feel capable of dealing with a risk, they are less likely to be fearful or worried by it. By helping children become more confident and competent users of the internet, including being able to face and deal with online risks, they will embrace more online opportunities without needing to be curtailed by restrictive mediation strategies.

Radicalization can originate from:

- Political purposes (for example, changing the form of governance, like abolishing the democratic system with elections that we have now and establishing a dictatorship).

- Social purposes (for example, when members of sport fan clubs strive to make a change or achieve a goal - to persuade sports fans of other clubs to support their club).
- Religious purposes (for example, when members of a particular religion want to impose a change that will make their religion dominant or exclusive).

Online the indoctrination process often occurs through conversations (chats), persuasion, influence, affection, or teaching organized in closed or isolated groups, forums, breakout rooms. 'Brought together by online journals, blogs, services and chat rooms, the participants enter forums where the extremist ideology becomes self-reinforcing' (Schaan and Phillips, 2011, p. 24).

The process of online violent radicalization via cyberspace in our country, as elsewhere, varies. Giving that this process is the person (target)-tailored, it may follow specific patterns and dynamics. Online violent radicalization on the internet and social media occurs through recruitment and indoctrination[6]. During the recruitment process, those who radicalize try to attract and ultimately isolate an individual (or a group) so that the person can affiliate, using the political and/or socio-economic grievances as a stepping stone for mobilization towards a change by using violent means.

Online violent radicalization usually begins with a selection that could be targeted and organized, or it could be spontaneous, i.e., self-selection when one is being selected through his or her behavior[7]. Using modern technologies and accustomed social behavior (i.e., being comfortable to use modern communication technologies and applications as conventional communication in the physical world).[8] For this purpose (selection), some of the well-organized malicious groups and individuals have constructed a

[6] UNESCO Background note Social media and youth radicalization in digital age, available online:
http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/background_social_media_radicalization.pdf
[7] Metodi Hadji-Janev Mitko Bogdanoski Dimitar Bogatinov (2020) "Toward safe and secure youth online: Embracing the concept of media and information literacy", KAS
[8] See for example: Postmes Tom & Brunsting Suzanne, (2002), "Collective action in the age of internet: Mass-communication and online mobilization", Social Science Computer Review, 20, 290-301, available at:
https://journals.sagepub.com/doi/10.1177/089443930202000306

profiling methodology. By scanning the online activities, collecting and processing data (analyzing the target's behavior), these groups or individuals initiate the selection process. There are several ways through which malicious groups and individuals can collect personal data from youth on the internet, including:

- Personal profile on any platform (Facebook, Twitter, Instagram, YouTube) for communication and video purposes. They can examine personal habits, buying behaviours, desires, hobbies and influencers, places, and pages of targeted person's interest and identify his/her vulnerabilities. The approach to collect this amount of data could be either by exploiting the weak online profile protection of people or as simple as sending a random friendship request on Facebook. Different methods to identify individuals vulnerable to extremist ideas may include certain hashtags on a social media post, etc.
- Collecting information through web pages and chat forums. People with malicious intentions have well-organized websites that are attractive and filled with content intended for certain individuals and groups likely to browse the content[9]. Information on these websites could be true, partially true, and completely false.[10] Websites or chat forums may or may not be linked to the content that is the ultimate goal. These sites often feature content that is prepared in advance to test the potential victim.[11] The collectors know how to measure individual reactions to certain content and form a strategy for approaching the identified target.
- Collecting information by watching video content. Like other techniques for behavior monitoring, online recruiters can exploit a person's browsing history to collect data. Most platforms have appropriate algorithms –programs that select what you are seeing on them. On some platforms, the videos posted have a list of individual views, with access to the viewers' profiles. One can be very

[9] Weimann Gabriel, (2015) "Terrorism in Cyberspace: The Next Generation", New York, NY: Columbia University Press/Washington, DC: Woodrow Wilson Center Press, ISBN: 978-0-231704496.

[10] Several independent researches confirm this, see for example: Brachman Jarret and Levine Alex, (April 13, 2011), "The World of Holy Warcraft", Foreign Policy, available at: http://foreignpolicy.com/2011/04/13/the-world-ofholy-warcraft/; or see: Behr Ines Von, Reding Anaïs, Edwards Charlie & Gribbon Luke, (2013); or: Sageman Martin, (2008), "Leaderless Jihad", University of Pennsylvania Press

[11] Busher Joel (2015), "What part do social networks play in radicalisation?", Radicalization Research, available at: http://www.radicalisationresearch.org/debate/busher-social-networks/

easily spotted if they watch videos with content intended to lure the new subscribers to a particular ideological worldview that calls on violence. Even though well-intended, some social applications' features are exploited by terrorist organizations, such as the YouTube guidelines on designing a video based on the profile/habits of desired viewers or followers. It is straightforward for recruiters to misuse this method for their own purposes.[12].

- Games. Games are another way that online mentors who are radical and searching for new followers can access personal information. Modern video games and gaming applications allow communication in a specially designed chat room from one player to another and, as such, create the perfect opportunity for predators. For example, hiding behind a game character to generate a discussion within the form of hate speech, which in turn can easily get used as a form of aggression against groups/individuals from the physical world.[13] According to some statistics, young people in our country prefer to play online, and 38% use the internet to play and download games, which is well above the European average of 34%.[14]

The CRPM Study Baseline Assessment "*Passage4Prevent: use of education to prevent youth online radicalization*" finds out that over half of the surveyed high school students very often access trolling, bullying, and online insults (52.7%) content, followed by violent content that is humorously portrayed (47.7%), or content showing physical assault, ignition and beating (39.9%) and hate speech that directly encourages people to behave violently or commit an act of violence (39.2%). Interestingly over 20% of surveyed students have confirmed that this type of violent internet content is shared by at least half of their friends. This suggests a widespread of violent content on the internet and high exposure of youth to violence. However, whether there is a risk for using this content to radicalize and accept violent extremist ideas should be further researched.

[12] See more at YouTube Creator Academy, accessed at: https://creatoracademy.youtube.com/page/lesson/discoverability-analytics

[13] Selepak, Andrew, (2010), "Skinhead Super Mario Brothers: An Examination of Racist and Violent Games on White Supremacist Web Sites" Journal of Criminal Justice & Popular Culture, 17(1), 1-47, available at: https://www.semanticscholar.org/paper/Skinhead-Super-Mario-Brothers%3A-An-Examination-of-on-Selepak/581e60a66b63bd58853d9cffb9304fb81f25314e

[14] Игор Петровски, (Јуни 29, 2018), „Младите и интернетот", Капитал

Once predators have located a target who uses any social media communication (Facebook, Twitter, Instagram, Snapchat, YouTube, etc.) on the internet, they move to the next phase of the recruitment: approach and isolation. The initial communication is usually in support of the victim's grievances to gain their confidence.[15] This means that "person" and "the group" can establish special online relations due to allegedly similar interests, habits, experiences, views, opinions, and attitudes. Much of these alleged similarities are preset and tailored based on the profiling process. More often, during this period, well-organized representatives of malicious groups present themselves as members who share similar views to the victim and thus latently invest in building up confidence in "the room" (chat room). The ultimate goal at this stage is to create a bond. For this purpose, they create closed chatrooms. This is where the isolation starts.

To advance and create further isolation, the victim may receive an exclusive offer. An example could be a proposal for certain privileges, i.e., becoming a member of the "special ones."[16] Another method to isolate the target could be providing access by recommendation in selected or special groups where all the "hot topics" occur. Discussions deliberately prepared beforehand may usually include topics such as rioting, changing the system, and hate speech against those who are different. In general, closed groups have rules based on the "members only" principles. The goal, at this stage, is to create a sense of belonging and for the victim to feel equal to the others. Earning trust may also include compensation. A person (victim of the online violent

[15] Weimann Gabriel, (2015)
[16] Weimann, Gabriel, (2010), "Terror on Facebook, Twitter, and Youtube", Brown Journal of World Affairs, 16(2), 45-54, available at: http://bjwa.brown.edu/16-2/terror-on-facebook-twitter-and-youtube/

radicalization) may be asked for a service (to do something) for which he/she will be rewarded. Once the trust is gained, the process of building a shared identity (indoctrination) begins.[17]

Certain wordings and phrases dominate isolated chatrooms during the indoctrination phase to encourage a general position on concrete issues. There is no rule about how much time passes from the selection process to indoctrination. It can be a lengthy process, but it can also happen very quickly. This process is done through manipulation –the belief that something that needs to be changed must be done, even if it entails the use of violence. Manipulation aims to produce distortion and abuse of beliefs, political ideologies, and ethnic and cultural differences (attracting simple

The CRPM Study Baseline Assessment "*Passage4Prevent: use of education to prevent youth online radicalization*" finds out that 44% of the respondents receive violent content via personal messages (inbox) or in chat rooms. While another 37% of the high school students, respondents to the CRPM survey, said that these types of violent content are also shared via created groups for sharing. This suggests that infrastructure and pattern of behavior that is used in online radicalization (isolation and indoctrination) are practiced and normalized among many high school students, which presents a risk for possible online radicalization.

global views that divide the world into "us versus them"), thus urging the victims to seek answers.[18] Phrases like "us," "we," "together," and "our" are used to enhance belonging, compensate for misfortunes and tragedies and encourage tailored behavior through inflicted loyalty, and the quest for "thrill and adventure" and "power and control" – substituting the real by the virtual world[19]. Based on profiling in the isolated group during the indoctrination process, the targets can express themselves, feel emotionally comfortable, and be protected. These groups create a circle of trust, and

[17] Some have called this process "identity fusion", see: Swann William Jr. & Buhrmester D, Michael (2015), "Identity Fusion", Psychological Science, Vol. 24(1) 52–57, available at: https://labs.la.utexas.edu/swann/files/2016/03/52-57.pdf

[18] Ibid.

[19] In the 2017 the Atlantic Initiative research, the so-called human touch is always identified as the beginning of the radicalization, in the edition of Azinovic, V (ed) (2017). "Between Salvation and Terror: Radicalisation and the Foreign Fighter Phenomenon in the Western Balkans. The Atlantic Initiative, p. 17, available at: http://www.atlantskainicijativa.org/bos/images/BETWEEN_SALVATION_AND_TERROR/BetweenSal vationAndTerror.pdf [20] In UNESCO's Manual these factors are singled out as pull factors. See more in UNESCO, (2017), op.cit.

when the victim feels safe, that individual is ready to be implanted with the previously perceived behavior as wrong, forbidden, or strange[20]. The resort to violence often becomes the moral justification against all odds that have put the victim on the opposite pole of the polarized spectrum in society.

Practice shows that the whole process described above may happen through "self-radicalization."[21] As mentioned earlier, pre-prepared manipulative websites can be found on the internet, which use written texts, videos, and music to distort the facts and exert influence toward violent radicalization or violent self-radicalization.

Based on an examination of 150 articles, of which only 18 were empirically derived studies, RAND has identified Al Qa'ida's media production house As-Sahab Foundation for Islamic Media Publication and their websites as such source. Self-radicalization can also happen when a random victim read literature, forums, and blogs from suspicious sources or stream videos, audio recordings, or songs with content that has the purpose to radicalize violently.

The literature review has identified the following five roles the internet has in promoting radicalization: (i) the internet creates more opportunities to become radicalized[22]; (ii) the internet acts as an 'echo chamber'[23]; (iii) the internet accelerates the process of radicalization[24]; (iv) the internet allows radicalization to occur without physical contact[25]; (v) the internet increases opportunities for self-radicalization[26]. The younger generation, is

[20] In UNESCO's Manual these factors are singled out as pull factors. See more in UNESCO, (2017), op.cit.
[21] More about this can be found in: Sageman Martin (2008), "Leaderless Jihad: Terror Networks in the Twenty-First Century", Philadelphia: University of Pennsylvania Press
[22] Pantucci 2011; Briggs and Strugnell 2009; Homeland Security Institute 2009; Weimann 2006; Precht 2008 who found that there is a correlation between jihadi web sites and propaganda on the internet and rapid radicalization in an empirical study of 242 European jihadists from 2001-2006.
[23] The internet has been described as an 'echo chamber' (Ramakrishna, 2010; Saddiq, 2010; Stevens and Neumann, 2009) or a 'mental reinforcement activity' (Silber and Bhatt, 2007) that provides supposed anonymity (Weimann, 2006) and a degree of protection and security from detection (Gray and Head, 2009), as well as provides acceptance: information is non-censured and non-hierarchical (Bartlett, 2011)
[24] Schmidle (2009) points to the role of chat rooms in particular in this acceleration effect, as extremists can exchange with like-minded individuals 24/7, regardless of borders
[25] 'Individuals have the comfort of accessing radical content from their own personal space instead of having to go through the inconvenience of physically 20 attending radical religious gatherings' (Yeap and Park, 2010, p. 2)
[26] According to RAND (2013) '*Radicalization in the digital era*' "what distinguishes self-radicalization from radicalization via the internet is that it takes place in isolation, and

particularly vulnerable to online radicalization as they accept online media much more naturally as part of their lives, and their social relationships than older generations do[27]. This means that the importance of face-to-face communication is declining, and online contacts are encountered with great trust, making policy interventions towards increased online safety to be a priority of any government.

implies a process whereby no contact is made with other terrorists or extremists, whether in person or virtually".

[27] KAS (2013) "*Online-Radicalisation: Myth or Reality?*", available online: https://www.kas.de/c/document_library/get_file?uuid=baca4877-ac6c-4df4-ae77-28b4ba2aafac&groupId=252038

The policy response to online radicalization

The challenge for governments and all stakeholders is to understand the range of factors in which social media may play a role so that responses are not misplaced or based on unsupported assumptions[28]. On this basis, it may be possible to identify appropriate steps to counter radicalization activity online and ensure appropriate legal, institutional, administrative and educational frameworks to respond to the threat in full compliance with the international human rights law. Steps should ensure that freedom of expression and privacy are free from arbitrary, unlawful, or disproportionate interference and can preserve the characteristics of the Internet being open, inclusive, and contributing to sustainable development and prosperity of modern society[29].

Despite the continuous fragile situation, the work on CVE in the country is limited, and on the online radicalization of youth even more. Analytica[30] studied the drivers of extremism encompass similar factors as those driving global extremism. The Islamic Community of Macedonia launched countering violent extremism (CVE) training for imams to encourage the community to find an alternative to embracing violence. The Berghof Foundation commenced with collaborative research and a dialogue initiative exploring why some communities are particularly affected while other communities may show greater resilience to radicalization. The Centre for Research and Policy Making researched on the perceptions of teachers and front-line workers on radicalization and violent extremism and built capacity through the development of guidelines, tools (checklists and protocols), and training workshops for early detection of radicalization. Women Without Borders instigated Mother's school project that aims to raise awareness on countering radicalism and enhance the competencies and capabilities of Macedonian mothers to deal with the phenomenon of radicalization in their relationship with children. The OSCE has trained teachers to become trainers on issues related to radicalization and violent

[28] Dan Shefet (2016) Policy options and regulatory mechanisms for managing radicalization on the Internet, UNESCO
[29] UN (2015) Plan of Action to Prevent Violent Extremism, available online: https://undocs.org/A/70/674
[30] Analytica, 2016 "Assessment of Macedonia's Efforts in Countering Violent Extremism"

extremism. The IOM has worked on the community level providing IC thinking youth training. CRPM has developed a training curriculum for high school students to increase their knowledge and skills for safe use of the internet to build resilience on online radicalization and developed a Manual for cyber security in schools to increase resilience to online radicalization.

In terms of policy framework, the National strategy of Republic of Macedonia for countering and preventing violent extremism[31] regulates relevant goals such as the Strategic goal 1.1. Strengthened institutional capacities; Strategic goal 1.4: Preventing radicalization via the Internet and Strategic goal 3.1: Established set of measures for early detection of radicalization of the National. The strategy is aligned with the United Nations Global Counter-Terrorism Strategy that among its action priorities provisions "the necessity to support "Education, skills development and employment facilitation" as a means to foster respect for human diversity and prepare young people to enter the workplace."[32] Similarly, it is streamlined with the EU Counter-Terrorism Strategy and the RAN Manifesto for Education – Empowering Educators and Schools[33].

More specifically, the Cybersecurity Strategy rightly points out that the cyberspace can be used for terrorism and identifies it as a possible national security threat, as part of the broader approach to cybersecurity principles[34]. However, it does not provision goals nor activities that specifically target youth, their capacity or resilience to radical ideas, or cyber-facilitated terrorism. The challenge to address online radicalization echoes the general challenges associated with the institutional capacities for e-governance. For example, an independent evaluation of cybersecurity capacities of the country, run by the World Bank and the Global Cyber Security Capacity Centre in 2018, asserted that "*It was not possible to obtain*

---

[31] Avalaible in macedonian at https://vlada.mk/sites/default/files/dokumenti/sne_nacionalna_strategija_2018.pdf

[32] The United Nations Global Counter-Terrorism Strategy (A/RES/60/288), adopted by the UN General assembly on 8 September 2006, is a unique global instrument to enhance national, regional and international efforts to counter terrorism. For more information visit: https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy

[33] RAN Manifesto for Education available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/docs/manifesto-for-education-empowering-educators-and-schools_en.pdf

[34] The Government of the Republic of North Macedonia, Republic of North Macedonia: National Cyber Security Strategy 2018 – 2022, p.12 available at: https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf

a clear picture regarding crisis management…" in the course of cyber threats.[35]

The Macedonian strategic plan for education 2020-2022[36] envisages strategic goal 2.2 Quality and inclusive secondary education that is in line with the Strategic document 'Reform in education and investment in innovations and information society technology,' but lacks priority, activities and key performance indicators related to increased resilience of high school students to online radicalization, nor mentions online safety of students.

The Concept for distance learning[37] of the Ministry of education puts some additional attention to the security of the technology used in distance learning, and the protection of personal data and privacy, as well as health protection and well-being of students and teaching staff and protection of the environment. However, the document does not assess online radicalization as a risk for implementing the distance learning system. Neither propose measures on how to increase safety on the internet and strengthen youth resilience to radical ideas that they can access on the internet. This is especially because the Eurydice Report[38] determines that most European education systems have incorporated digital competencies as a horizontal theme. Still, in many countries of Eastern Europe, the issues of online safety and building youth resilience are treated with a more holistic approach as part of a comprehensive strategy. In contrast, inWestern, Central, and North Europe, these issues are tackled with a separate strategy. In Macedonia, the digital competencies are acquired through two courses, one compulsory and one elective, but online safety issues are merely covered with the curriculum.[39]

---

[35] World Bank & Global Cyber Security Capacity Centre, (2018), "Cybersecurity Capacity Review, Former Yugoslav Republic of Macedonia (FYR Macedonia)", Wordl Bank, p.9 available at: https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

[36] MON (2019) Strategic plan 2020-2022, available on internet: https://mon.gov.mk/stored/document/Strateski%20plan%20%202020-2022.pdf

[37] MON (2020) Concept for development of distance learning system in the primary and secondary schools https://mon.gov.mk/content/?id=3262

[38] Eurydice (2019) Digital Education at School in Europe, available on line: https://eacea.ec.europa.eu/national-policies/eurydice/content/digital-education-school-europe_en

[39] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatika-I_SSO-trigodishno-mkd.pdf

In fifth grade, the Macedonian education system of primary education envisages the course *Work with computer and basics to computer programming,* which according to the teaching program[40] includes only one content related to online safety: discussion for internet communication and safety issues related to internet communication.

In sixth grade, the Macedonian education system of primary education envisages the course *Informatics,* which has seven goals according to the teaching program,[41].Four are related to computer science; one is information technology-related and two focus on digital competencies. One of the digital competencies objectives that are most relevant for building online resilience is to use the technology ethically and responsibly and safely to keep personal information. In this regard, the curriculum provisions that students will determine safety rules for the classroom where the informatics class takes place and discussion with students will be stirred to determine ethics in computer use and possible misuse. In terms of internet safety, also a discussion of safety issues in internet communication is planned for the second semester. However, assessment of information, data, and digital content and their risk for online radicalization is not provisioned.

In seventh grade, the course *Informatics*[42] is a compulsory course that encompasses 5 classes for online living that indirectly tackle online safety. Indirectly, the curriculum does not include content on safety and competencies for assessing digital content but rather builds skills for creating web pages, blogs etc. It is recommended, though, for the online living topic resources that offer recommendations on the safe use of the internet to be used as teaching materials such as the websites of: http://bezbednonainternet.org.mk, www.dzlp.mk, and www.iSafe.org.

In eighth and ninth grade Informatics is not offered as a compulsory or elective course in the Macedonian primary education system.

In secondary education, the students in gymnasium, have *Informatics* as a compulsory course in the first year, which introduces them to hardware, software, and the basic introduction to programming[43], but as no content in

[40] https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Rabota_so_kompjuter_i_osnovi_na_programiranjeto-V_odd-2020.pdf
[41] https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Informatika-VI_odd-2020.pdf
[42] https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Informatika-VII_odd-2020.pdf
[43] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatika-I_SSO4-mkd.pdf

the curriculum that is related to online safety and digital competences that might decrease vulnerability to online radicalization. In the second year, this course is offered as an elective together with information technology as a course[44], while in the third[45] and fourth years[46] as a compulsory programming is offered. None of the curricula includes digital competencies and in particular issues related to security such as protection of devices, protection of personal data and privacy, protection of health and wellbeing as required by the Digital Competences Framework for Citizens of the European Commission[47].

The Digital Competences Framework has been adopted in 2016 and updated in 2018 foresees 5 key areas measured and monitored by the European Union: (i) digital literacy; (ii) communication and cooperation; (iii) digital content development; (iv) safety; and (v) problem-solving. From the analysis of the curriculum presented above, it seems that the Macedonian primary education is more directed towards building skills and enhancing knowledge on digital literacy as well as communication and cooperation; while the secondary on digital content development and, to some extent, problem-solving, but what is thoroughly missing in both education levels is focus on safety. Considering that the results of the CRPM Study Baseline Assessment "*Passage4Prevent: use of education to prevent youth online radicalization*" shows that about thirty percent of the high school students in the studied municipalities are sharing personal information with strangers over internet communication[48], such as name, age, email addresses, school, personal photos, etc., and that still large portion of them said that rarely or never check the reliability of the information on the internet (40.7%), thus making them vulnerable to fake news, disinformation, radical ideas on the internet. This focuses on online safety, a priority that needs to be tackled with both legislative/curriculum changes,

[44] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatichka_tehnologija-II_GO-mkd.pdf
[45] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Programski_jazici-III_GO-PMA-mkd.pdf
[46] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Programski_jazici-IV_GO-mkd.pdf
[47] European Commission. *Digital Competence Framework for Citizens* (DigComp 2.0). 2018. https://op.europa.eu/en/publication-detail/-/publication/bc52328b-294e-11e6-b616-01aa75ed71a1/language-en
[48] The survey shows, 32.6% of the respondents said that they have shared their name with someone they met only online, 31.8% shared their age, 29.5% shared information about the school they study in, while 23.8% have shared their photos. 21.1% of the high school students have shared information with someone they only met online about where they do out.

capacity building, and school policy type of responses. The ***DigiComp2.0*** Framework can serve as a roadmap to achieving this objective.

In this process, students and their families, and whole of society, are beneficiaries, whereas schools and teachers/educators are stakeholders who act as agents. Teachers in particular need to be directly targeted as the CRPM Study Baseline Assessment "*Passage4Prevent: use of education to prevent youth online radicalization*" shows that when students feel threatened while online, 61% of them will speak to their parents/guardians, 20% choose to speak with a friend, while 16% will report the threat to the police, and only 1% said that they would speak with teachers/professors if they feel threatened online. This suggests lack of trust in teachers or their role in building resilience and digital competence is not visible and recognized by students. This might be because of a lack of competencies or lack of school policies for ensuring online safety. To this end, the high school students who participated in the CRPM survey think that their parents have more knowledge (79% of the respondents), than the teachers, for whom 63.6% of the respondents said to have somewhat knowledgeable about the internet and its capabilities. There is a high percentage of students (16.7%) who think that their teachers lack knowledge. Therefore, increasing teachers' competencies should be one important section of the comprehensive policy for enhanced resilience for online radicalization. The European Framework for Digital Competences of the educators/teachers[49] can serve as a guiding policy document for that objective. The ***DigiEduComp*** Framework encompasses six areas where teacher's competencies need to be built: (i) professional engagement; (ii) digital resources; (iii) education and learning; (iv) assessment; (v) student support and (vi) improvement of the students' digital competences in terms of information and media literacy, communication, content development, responsible use of internet and problem-solving.

What is more, except for one school in Skopje, the remaining 41 schools in the project did not have a digital safety policy either any measure implemented towards that goal. Regarding whether there should be a policy/guideline on the use of smartphones/devices and the internet in the school agreed between teachers, students, and parents/guardians that will include guidelines for certain aspects of the use, 73% of the high school students/respondents in the CRPM Study Baseline Assessment

[49] European Commission. *Digital Competence Framework for Educators*. 2017, available online: https://ec.europa.eu/jrc/en/digcompedu

"*Passage4Prevent: use of education to prevent youth online radicalization*" would approve such guideline in general. By specific aspects that should be covered by the guidelines, the support is: a) online content protection (78.8%), b) not sharing personal information and data (70.3%) c) Internet behavior regarding protection against cyber-violence (78.8%) d) checking information (66.9%). Therefore, the Ministry of education should undertake an initiative to develop and adopt school policies for online safety to decrease vulnerability to online radicalization. To this end, the Digitally Competent Educational Organizations Framework[50] can serve as a guideline as it encompasses seven key elements and the SELFIE tool[51] with which the schools can develop their digital strategies to improve teaching-learning and online safety. The tool is offered in the Macedonian language as well.

Teachers, as parents, are important because they can oversee the online activities of their students/children. In the CRPM Study Baseline Assessment "*Passage4Prevent: use of education to prevent youth online radicalization*", 69.3% of the respondents said that they are friends with their teachers, and 85.9% are friends with their parents on the social networks. Without interfering with the freedom of thought and speech in the online engagement of their students, teachers can play a monitoring role in the very early stages of radicalization by observing the online engagement of their students. The shared content and online comment discussions can be some of the indicators of radical ideological changes in students. Teachers can also create digital space for the youth to disengage them from further steps to radicalization. What is more, in social media engagement, teachers that are motivated and want to be active agents of change can use their platform to share alternative/ positive narrative content (pictures, videos, and blogs) that promote messages against radicalization.

[50] https://ec.europa.eu/jrc/en/digcomporg
[51] Schools go digital https://ec.europa.eu/education/schools-go-digital_mk

Towards an Online Safety Policy

To set up an online safety policy, one must implement a comprehensive approach that is consisted of legislative changes, professional development requirements, and policy response on the school level. The following are recommendations that the Ministry of education, as a policymaking body, the Bureau for Development of Education as a teacher training and curriculum development body, and the schools as service delivery organizations can take in the coming period so that resilience to online radicalization is built.

Legislative response

Law on Primary education[52] and the Law on secondary education[53] do not provide any online safety requirement, privacy, or personal data protection except for the data gathered and kept by the schools themselves (the so-called educational statistics). To this end, legislative changes of both laws are needed to address student's safety online, the requirements every school needs to fulfill to provide a digitally safe environment for learning, and the digital competencies the teaching staff should obtain. To this end, the ***DigiComp2.0*** Framework, the ***DigiEduComp*** Framework, should be used as roadmaps for reform. Furthermore, the exam for the Director of the school should be revised to include in the Module: Theory of organization where the school online safety policy will be one of the issues tackled as per the ***DigiCompOrg*** Framework.

[52] https://mon.gov.mk/download/?f=zakon%20za%20osnovnoto%20obrazovanie%208.10.docx

[53] https://mon.gov.mk/download/?f=Zakon%20za%20srednoto%20obrazovanie%20%2008.10.2020.docx

Professional development and curriculum response

As the analysis above showed, the curriculum lacks important online safety content. The Bureau for Development of Education should develop it and included it in compulsory courses. It is especially recommended to add content related to security such as protecting devices, protecting personal data and privacy, and protecting health and wellbeing. Radical content should be used in exercises for building critical thinking skills, while when digital content development is thought alternative positive narratives creation should be stimulated.

Digital literacy of teaching staff should be raised through training but also the active role of teachers as agents of online safety should be prescribed in the school policy for online safety. This will increase the visibility of teachers, and their role be recognized by students who currently, as research shows, is very low. In this process, choosing a teacher as an e-safety lead would help to implement the policy in each school. Once the school level e-safety policies have been developed schools should consider getting the rest of the staff base on board by explaining the importance of e-safety and organizing training around their own safe and responsible use of the Internet and the school's e-safety policies.

E-safety policy response on school level

Each school should develop its e-safety policy, either using the SELFIE tool or following the checklist provided in Annex 1 of this paper. The policy should include designated responsible teachers for the coordination and implementation of the e-safety policy. However, since it’s a school policy discussion around the general principles of e-safety as well as what steps to take if an e-safety issue arises could be included in regular teaching staff meetings and in the master class together with students. Having e-safety on the agenda of teacher-parent meetings and school council meetings will increase the visibility of the school e-safety policy but will contribute to more enhanced resilience to online radicalization. The reason would be to provide explanations of why schools are interested in e-safety at school and in pupils' homes and to increase trust in teachers by students.

Schools should address e-safety at an organizational level. To this end, each school should have virus protection, encryption of personal data, and safety school website to be secured and not include personal information about staff or pupils and identifiable images. Then, the school should choose between locking content that is harmful or using fewer filters in place to assist students in managing online risks rather than avoiding them at school and being exposed to them elsewhere.

The school policy should include using tools such as the Home-School Agreement, which is signed by the parent, student, and teacher (please see example in Annex 2), and the Staff user agreement, which outlines what is appropriate and professional for staff in terms of their online behavior. The feedback from the teachers and students on take home agreements, promoted within the project implemented by CRPM is very positive, as both sides stated that it helped them further discuss the online safety at school and home, and it raised their awareness on the cyber safety in general.

Finally, schools should also take into account Acceptable Use Policies and consider the merits of them being updated on an annual basis so that any new digital concerns can be integrated. The Acceptable Use Policies usually include rules and advice for students on: turning off the screen and informing an adult if they find anything unpleasant or disturbing online; touching files that are not their own; being respectful to other people online; sending abusive or inappropriate text messages; giving out personal details that might identify them or their location; placing photos of themselves online; denying access to unknown individuals; blocking unwanted communications; and privacy settings, security, and passwords.

Annex 1: Checklist for E-safety School Policy

	Definitely in place	Needs review and attention	Not in place
A dedicated e-safety lead			
An e-safety policy which is regularly updated			
Acceptable use policy for pupils			
A staff user agreement			
Managed systems			
Up-to-date regular staff training			
E-safety as an agenda item in school meetings			
Training for all staff groups			
Take home contracts			
E-safety on the agenda in parent-teacher meetings			
E-safety on the agenda in school council meetings			

Annex 2: Take home contract

This agreement regulates the use of smart devices, computers and internet in the family of _____.

The rules set out in this agreement apply to family members stated below:

Parents _____and_____
children_____and _____and _____

The rules set in this agreement also apply to guests in the family home who use the internet.

Computers, smart devices and internet will be used to inform, learn and communicate with the best of intentions and in a way that will not harm anyone.

Computers, smart devices and internet will be used within a reasonable time of day and for the duration specified by the parents.

Websites that have inappropriate and violent content that may disturb children are not allowed. Parents should be notified when such content is found.

Inappropriate and violent content is not allowed to be downloaded and saved on a computer or smart device. If this happens, parents should be notified.

All profiles that children use on social networks should be reported to parents.

Using secret and false profiles on social media is not allowed.

Do not share personal information and data on suspicious websites or with strangers on social media.

Avoid physical meetings with online people that are unknown. If there is a proposal for such a meeting, the parents should be informed, and if necessary, the meeting must be in the presence of a parent or adult in a public place.

Do not share phone numbers with strangers online and answer calls from strangers. If there is such a call or request for a call, notify the parents.

Internet or social media communication should be polite, without offensive words and content. The use of such words and content should be reported to parents.

Downloading and installing software without parental permission as well as illegal content from websites is not allowed.

Compliance with these rules also applies when using internet elsewhere (at a friend's, internet cafes, schools, public spaces, etc.)

Failing to comply with these rules will activate the sanctions below: [54]

_____

_____

_____

CHILDREN'S SIGNATURES:	PARENTS SIGNATURES:
_____	_____
_____	_____
_____	

[54] Examples of sanctions include: taking away the computer or smart device over a determined period of time or indefinitely, ban to use the internet, limiting the time spent online, etc, depending on the gravity of the breach.

Annex 3: Staff User Agreement [55]

Please complete, sign, and date this Staff Use Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document. The key obligations and responsibilities are:

- All ICT use must be appropriate to the school environment
- Passwords will be kept confidential
- The principles of confidentiality, privacy and copyright apply.

If you have any queries about the agreement, you are encouraged to discuss them with the online safety manager or the principal before you sign. Once signed, this form should be returned to the school office to be passed on to the online safety manager for filing with staff records.

A copy of the signed form will be supplied to you.

Please tick one -

❑ I believe that I have sufficient knowledge to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/devices.

❑ I require additional training/professional development in order to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices.

[55] This is an example of staff user agreement from New Zealand, available online: http://www.cybersafety.org.nz/kit/Use%20Agreements/agreements/staff_ua.html

Use agreement

I have read and am aware of the obligations and responsibilities outlined in this Staff On line safety Use Agreement document, a copy of which I have been advised to retain for reference. These obligations and responsibilities relate to the online safety of students, the school community and the school environment.

I also understand that breaches of this Staff On line safety Use Agreement will be investigated and could result in disciplinary action, and where required, referral to law enforcement.

Name: .....

Role in the school: .....

Signature: .....

Date: .....

Annex 4: Acceptable Use Policies [56]

Aim

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege.

It is envisaged that school and parent representatives will revise the AUP regularly. Before enrolling, the AUP should be read carefully to ensure that the conditions of use are accepted and understood. It is assumed that the parent accepts the terms of the AUP unless the school is specifically notified.

School's Online Safety Policy

The school employs a number of tools within its online safety policy.

General

- Internet sessions will always be supervised by a teacher.
- The school will regularly monitor pupils' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- It is important that parents/guardians and pupils are aware of our Anti Bullying Policy in relation to social media;

Isolated or once-off incidents of intentional negative behavior, including a once-off offensive or hurtful text message or other private messaging, do not

[56] This is an example of the Powerstown Educate Together National School Acceptable use policy from Ireland

fall within the definition of bullying and should be dealt with, as appropriate, in accordance with the school's code of behavior.

However, in the context of this policy, placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behavior

World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only during class time. The class teacher will vet all web sites.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicize personal information.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's acceptable usage policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email / Google Drive / Internet Chat

- Students must sign a written take-home agreement annually, with parents and class teacher, prior to accessing school email accounts.
- If a student receives any inappropriate emails, he/she should inform class teacher and a parent/guardian.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers, pictures or passwords.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.

- Students will not have access to chat rooms, discussion forums, messaging or other electronic communication forums.

Web 2.0

With the advent of Web 2.0, the Internet has become a two-way communication system for the school and the wider community. Services such as Scribd, Class Dojo, Facebook, Wordpress, Twitter and other social media are being used by the school to communicate with parents and for parents to communicate with the school. These services, form part of our web services and all content that is placed on these services falls under this policy. For example, any content on the school's Scribd account follows the same safety rules, e.g. the showing of photographs, video, etc.

- Many social media sites have minimum age requirements. While the school will not monitor this, we would advise parents to not allow their children to have personal accounts on Facebook, Twitter, etc. until they are the appropriate age. Many social media sites will be used by teachers in class, for example, Twitter. However, all interactions will be under the supervision of the teacher.
- Parents and guardians are encouraged to regularly check their child's online activity / digital footprint. Parents are encouraged to check social media apps (e.g. Facebook, Snapchat, Viber, WhatsApp, Instagram etc) on mobile phones and electronic devices to ensure they are aware of their child's online interaction with others and approve of it.
- Please do not "tag" photographs or any other content, which would identify any children or staff in the school.
- If you are uploading a photograph, please ensure that it does not identify the child in any way. Please make sure photograph size is kept as small as possible (no bigger than 800x600 pixels).
- Please ensure that online messages and comments to the school are respectful. Any messages written on social media are treated in the same way as written messages to the school.
- Avoid any negative conversations about children, staff or parents on social media accounts.
- Please do not add advertisements to our wall without prior permission of the principal.
- Failure to keep the above rules will result in a permanent ban to our social media accounts.

School Website

- Please note that the following points apply to the school's web site and social media profiles, including but not limited to Facebook, Twitter, YouTube, Scribd and Google+
- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- Website using facilities such as guest books, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details.
- The publication of student work will be coordinated by a teacher.
- Pupils' work will appear in an educational context on Web pages.
- The school will endeavor to use digital photographs, audio or video clips of focusing on group activities. Photographs, audio and video clips will be used. Video clips will not be password protected.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the last name of individuals in a photograph.

Mobile Phones / Electronic Devices

- Usage of mobile phones/ electronic devices must be in adherence to the Mobile Phone / Electronic Devices Policy.
- The school acknowledges the usefulness and practicality of mobile phones / electronic devices and recognizes their potential as an educational resource.
- Many features on mobile phones / electronic devices such as Organizer (calendar, calculator, convertor etc) Applications (voice recorder, stopwatch, image editor, video recording) or even Alarms are very useful and may be used under the direction of the class teacher. If and when any such activities take place parents will be notified in advance.

- Pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class is in direct breach of the school's acceptable usage policy.
- Pupils sending nuisance text messages is a direct breach of the school's acceptable use policy.
- The unauthorized taking of images with a mobile phone camera or electronic device, still or moving is in direct breach of the school's acceptable usage policy.