

Passage4prevent:



**Përdorimi i arsimit për
ta parandaluar radikalizimin në internet të të rinjve**

Përgjigja ndaj radikalizimit në internet: Drejt politikës së arsimit mbi sigurinë në internet

Marija Risteska, Metodi Haxhi-Janev dhe Samet Shabani

Ky botim u realizua me projektin “Passage4prevent: Përdorimi i arsimit për të parandaluar radikalizimin e të rinjve në internet”

Passage4prevent:



Përdorimi i arsimit për
ta parandaluar radikalizimin në internet të të rinjve

Për botuesin: Qendra për Hulumtim dhe Hartim të Politikave

Autorë: Marija Risteska
Metodi Haxhi-Janev
Samet Shabani

Dizajni: Omni Grup

Ky botim është bërë me mbështetjen financiare të Bashkimit Evropian. Përmbytja e tij është përgjegjësi e vetme e Qendrës për Hulumtim dhe Hartim të Politikave dhe nuk i pasqyron domosdoshmërisht pikëpamjet e Bashkimit Evropian dhe as të Hedayah

Shkup, 2021

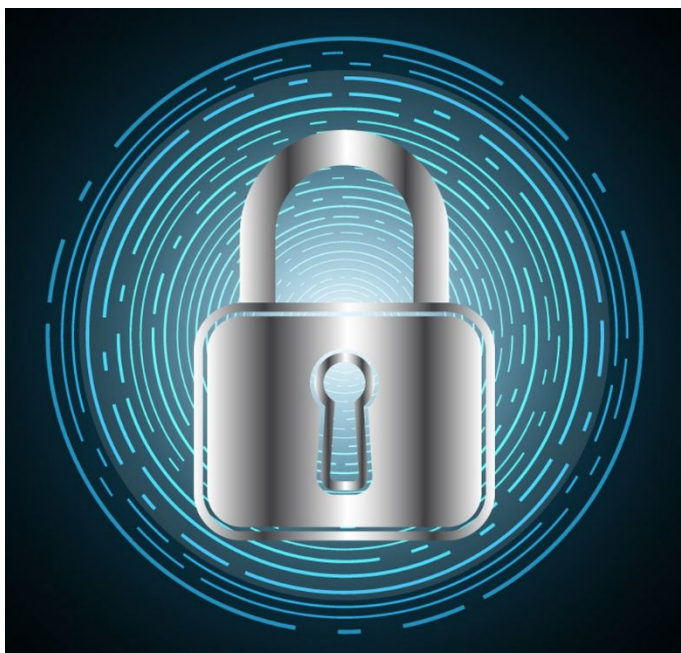
Përmbajtja

Përmbledhje	4
Hyrje	5
Pse të përqendrohemi në sigurinë në internet?	7
Si funksionon radikalizimi në internet?	9
Përgjigja e politikës ndaj radikalizimit në internet	17
Drejt një Politike të Sigurisë në internet	25
Përgjigja legjislative	25
Zhvillimi profesional dhe përgjigja e kurrikulës	26
Përgjigja e politikës së sigurisë elektronike në nivelin e shkollës	26
Shtojca 1: Lista e Kontrollit për Politikën e Shkollës për Siguri Elektronike	28
Shtojca 2: Kontrata e marrë në shtëpi	29
Shtojca 3 Marrëveshja e Përdoruesit të Kuadrit	31
Shtojca 4 Politikat e Përdorimit të Pranueshëm	33

Përmbledhje

Digjitalizimi i arsimit është një proces që ka vazhduar me dekada, dhe kriza Covid-19 ka përshpejtuar ritmin e saj, duke e vendosur sigurinë në internet në arsim si një temë prioritare të reformës për çdo vend. Maqedonia e Veriut përballet me radikalizimin onlajn si një rrezik i shoqëruar me mungesën e kornizës së politikave që trajton çështjet që lidhen me sigurinë e internetit në shkollë, duke e bërë çështjen kryesore me interes për këtë letër që i përgjigjet radikalizimit në internet përmes politikës arsimore mbi sigurinë në internet një domosdoshmëri absolute për hartuesit e politikave arsimore.

Punimi synon të informojë mbi politikat dhe prezantimin e politikës arsimore të sigurisë në internet. Për atë qëllim, së pari paraqet problemin e radikalizimit në internet dhe faktorët që po kontribuojnë në problem, duke e lidhur atë me prova se sa janë përhapur këta faktorë në mesin e nxënësve të shkollave të mesme nga Shkupi, Tetova, Gostivari, Velesi, Kumanova dhe Shtipi. Së dyti, punimi ofron një analizë të politikave të sigurisë kibernetike, edukimit dhe parandalimit nga korniza e politikave të ekstremizmit të dhunshëm dhe sesi këto korniza i përgjigjen situatës, duke i zbutur dobësitë e nxënësve të shkollës së mesme për t'u ekspozuar ndaj faktorëve që kontribuojnë në internet dhe fenomenet e radikalizimit. Më në fund, dokumenti i politikave paraqet zgjidhjen që propozohet të jetë e shumëfishtë, duke e përfshirë përgjigjen legislative, përgjigjen e politikave në nivelin e shkollës, dhe ndërtimin e kapaciteteve, si dhe vetëdijen e nxënësve, mësuesve dhe prindërve. Së fundmi, dokumenti i politikave rekomandon disa mjete që mund të përshtaten me nevojat e organizatave arsimore dhe komuniteteve për të siguruar politika të përshtatshme të sigurisë në internet që do të parandalojnë radikalizimin onlajn.



Hyrje

Interneti, në veçanti media sociale, përdoret si një kanal, jo vetëm për të promovuar dhe angazhuar, por edhe si një strukturë komanduese për radikalizimin që mund të çojë në ekstremizëm të dhunshëm. Shpesh ky promovim glorifikon dhunën, duke tërhequr dhe ndikuar në shumë njerëz, përfshirë fëmijët dhe në raste ekstreme, duke i radikalizuar ata. Gjithashtu, ndodh një prirje tjetër e promovimit të vuajtjeve që shkakton ndjeshmëri dhe personifikim me kauzën (veçanërisht tek gratë) që përfundimisht mund të çojë në adoptimin e sjelljes radikale për të arritur objektiva të caktuara.

Pasja e një strategjie për sigurinë në internet në arsim, duke e marrë parasysh që të rinjtë e kalojnë pjesën më të madhe të kohës në shkollë, është, pra, një përparësi për çdo vend. Prandaj, vendet që kanë përjetuar fenomenet e luftëtarëve të huaj duhet madje t'i japin përparësi përpjekjeve për vendosjen e standardeve të sigurisë në internet, të ndërtojnë kapacitete dhe të rrisin vazhdimisht ndërgjegjësimin.

Ky dokument politikash ka për qëllim të informojë zhvillimin e politikave arsimore drejt sigurisë në internet. I njejtë është zhvilluar duke përdorur metoda të shumfishta: (i) hulumtimi i nivelit të lartë, (ii) intervistimi ballë për ballë i aktorëve kryesorë të cilët për qëllimin e këtij punimi mbeten anonimë dhe (iii) gjetjet kryesore të të dhënave nga vlerësimi fillestar i CRPM në përdorimin e arsimit për të parandaluar radikalizimin e të rinjve në internet.¹

Punimi ndjek një metodologji të politikës për zgjidhjen e problemit. Së pari, ai paraqet problemin, radikalizimin në internet dhe fushën e tij në Maqedoninë e Veriut, pastaj ofron një analizë të politikës se si e adreson këtë problem. Në përfundim, punimi ofron rekomandime se si politika arsimore dhe politika shkollore mund të përmirësohen për të zgjidhur problemin.

¹ Sondazhi u krye nga shkurti deri në mars të vitit 2020, në komunat e Kumanovës, Shtipit, Velesit, Tetovës, Gostivarit dhe Qytetit të Shkupit, në një ekzemplar përfaqësues prej 756 nxënësish. Raporti është në dispozicion në: 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=IwAR1wLdERnOQPbLhlSc3X6BEP4FumfT9fXYZvZdYCbXTii xEKAX-SBh7qL7Q

Pse të përqendrohemi në sigurinë në internet?

Rreth 250,000 nxënës që nga marsi i vitit 2020 ndjekin arsimin në internet dhe kontribuojnë në trendin në rritje të përdorimit të internetit nga të rinjtë në Republikën e Maqedonisë së Veriut (në tekstin e mëtejme Maqedoni), që sipas Entit Shtetëror për Statistikë arrin në 99.5% të të rinjve të moshës midis moshës 15 dhe 24 vjeç në vitin 2019². Adoleshenca është një kohë e karakterizuar me idealizëm, me një tendencë drejt të menduarit gjithçka ose asgjë. Për më tepër, ata kalojnë afërsisht 6 orë në ditë në internet, kryesisht duke përdorur rrjete të mediave sociale dhe duke parë video³.

Nxënësit e shkollës së mesme janë shumë të varur nga moshatarët për një ndjenjë të mirëqenies, që kanë nevojë të ndihen sikur janë pjesë e një grupi - megjithatë gjithashtu dëshirojnë të shihen si unikë dhe 'monedha' e tyre janë pëlqimet dhe vlerësimet. Vlerësimi fillestar i CRPM ***"Passage4prevent: Përdorimi i arsimit për të parandaluar radikalizimin në internet të të rinjve"*** ofron gjetje shtesë për nxënës të shkollave të mesme në Gostivar, Kumanovë, Shkup, Shtip, Tetovë dhe Veles duke vërejtur se 99% e nxënësve kanë qasje në internet në shtëpinë e tyre, jashtë prej të cilave, 85% thanë se kanë qasje gjithmonë, ndërsa nuk ka rregulla për përdorimin e internetit në 74.4% të shtëpive. Pothuajse gjysma e nxënësve pranojnë mbikëqyrjen e prindërve (44,1%), ndërsa më shumë se gjysma (55, 9%) e nxënësve mendojnë se mbikëqyrja ose kontrolli i prindërve nuk është i nevojshëm.

Shkollat në anën tjetër nuk kanë politikë për përdorimin e sigurt të internetit dhe nuk përfshijnë në kurrikulën e tyre edukimin dhe ngritjen e vetëdijes për çështjet e privatësisë dhe sigurisë kibernetike. Këto rezultate tregojnë se në 26.4% të nxënësve të shkollës së mesme ndonjëherë e ndajnë

² Enti Shtetëror për Statistikë, Baza e të dhënave MAKStat, në dispozicion në internet në: 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, fq. 16, në dispozicion në internet në: <http://library.fes.de/pdf-files/id-moe/15266.pdf>

emrin e tyre të përdoruesit dhe fjalëkalimin me miqtë e tyre, dhe 33.8% nxënës të shkollës së mesme duke përdorur automatikisht 'opcionin e ruajtjes' për llogaritë e tyre në shfletuesit e internetit. Prandaj, vetëm 10% e nxënësve të shkollës së mesme të anketuar ndihen të pasigurt në internet, dhe 8.5% kanë pasur përvoja të këqija personale.

Duke e marrë parasysh se vendi e ka përjetuar procesin e radikalizimit të rinisë, i cili ishte veçanërisht i dukshëm gjatë konfliktit sirian, përmes fenomeneve "luftëtarë të huaj terroristë" (mbi 140 luftëtarë), kryesisht nga Shkupi (Çairi, Gazi Baba), Kumanova, Likova, Tetova; dhe procesi i vazhdueshëm i kthimit të tyre në vend (83 janë riatdhesuar dhe gjykuar sipas nenit të Kodit Penal 322a i cili është miratuar në vitin 2014, si dhe 23 persona të tjerë që nuk janë gjykuar pasi kthimi i tyre ka ndodhur para ndryshimeve të ligjit dhe kriminalizimi i aktit për të mobilizuar dhe shërbyer në një ushtri të huaj). Luftëtarët e huaj të mbetur dhe familjet e tyre pritet të riatdhesohen së shpejti, për këtë arsye Qeveria ka miratuar një Plan Kombëtar të Veprimit për Rehabilitimin, Rocializimin dhe Riintegrimin e luftëtarëve të huaj dhe familjeve të tyre. Për më tepër, marrëdhëniet ndëretnike në vend midis komuniteteve vazhdojnë të jenë të tensionuara sidomos në disa pjesë të vendit, ku grupet ekstremiste janë akoma të pranishme dhe aktive, të cilat janë të gatshme të përdorin dhunën për arritjen e qëllimeve të tyre politike. Disa nga këto procese po ndodhin në internet, pasi përpjekjet e Moonshot CVE për t'iu përgjigjur një trendi në zhvillim të radikalizimit në internet kanë përfshirë një fushatë gjithëpërfshirëse onlajn dhe oflajn për të luftuar mesazhet e organizatave terroriste ndërkombëtare dhe ekstremiste të dhunshme në vend ndërsa veprojnë për të parandaluar rreziqet nga mesazhet ekstremiste përmes aktiviteteve që synojnë drejtuesit që kontribuojnë në këto rreziqe, veçanërisht tek të rinjtë.⁴ Sidoqoftë, nevojitet një strategji dhe politikë më gjithëpërfshirëse për monitorimin, kontrollin, parandalimin dhe promovimin e praktikave të sigurta në internet.

⁴ Rekrutimi i Organizatave kundër ekstremizmit të dhunshëm në Gjeorgji, Azerbejxhan dhe Maqedoni, në dispozicion onlajn në: <https://www.ph-int.org/program/242/>



Si funksionon radikalizimi në internet?

Koha e shtuar e kaluar në internet do të thotë që fëmijët prezantohen vazhdimisht me zgjedhje morale dhe etike si prodhues dhe konsumatorë të përmbajtjes (Dita, 2016), dhe tashmë janë vendimmarrës aktivë në proces. Në Maqedoni, përderisa luftëtarët e huaj ishin burgosur pasi aktiviteti i tyre u kriminalizua, ekzistojnë prova që ata janë akoma aktivë në internet dhe se faqet e tyre në FB janë shumë të popullarizuara në mesin e të rinjve. Prandaj, nxënësit e shkollës së mesme hasin më shumë rrezik, por atyre u mungojnë aftësitë, strategjitë e përballimit dhe qëndrueshmëria për t'u përballur. Nëse ata nuk trajnohen, dobësitë e tyre (me dobësi në internet të shpjeguar në përgjithësi nga faktorë të ngjashëm me ata që llogarisin cenueshmëri dhe rrezik jashtë linje) do të mbeten.

Është një argument i mirëpranuar që teknologjitë moderne të tilla si interneti dhe aplikacionet e komunikimit në internet janë një shpatë me dy presa. Këto teknologji ofrojnë shumë përparësi, por gjithashtu paraqesin shumë rreziqe. Faktorë shtetërorë dhe joshtetërorë po abuzojnë me këto teknologji për të çuar më tej objektivat e tyre, duke turbulluar kështu kufijtë midis avantazheve dhe rreziqeve që tejkalojnë kufijtë e sigurisë dhe sigurisë individuale (emocionale/psikologjike, ekonomike) përmes përdorimit të hapësirës kibernetike nga organizatat terroriste në një nivel më të ulët në fund dhe nga agjencitë e sigurisë kombëtare në një fund më të lartë. Prandaj, mjetet dhe mediumet që sigurojnë mallin dhe mirëqenien e shoqërisë sonë janë bërë vektorë kërcënimi.

Ndërtimi i përpjekjeve të rezistencës digjitale synon forcimin e aftësisë së fëmijës për të identifikuar dhe interpretuar drejt ndikimin dhe pasojat e rrezeve të ndryshme në internet për radikalizimin dhe për të zhvilluar si aftësitë teknike ashtu edhe ato emocionale për t'u marrë me propagandën dhe rekrutimin ekstremist. Kështu, kërkohet të ndërtohet njohuria dhe ndërgjegjësimi i nxënësit të shkollës së mesme rreth rrezeve në internet pa u përqëndruar ekskluzivisht në rreze të veçanta ose të menjëhershme. Vandoninck, d'Haenens dhe Smahel (2014) zbuluan se kur fëmijët ndihen të aftë të përballen me një rrezik, ka më pak të ngjarë të frikësohen ose shqetësohen prej tij. Duke ndihmuar fëmijët të bëhen përdorues më të sigurt dhe më kompetent të internetit, duke përfshirë aftësinë për t'u përballur dhe trajtuar rreze në internet, ata do të jenë në gjendje të përqafojnë më shumë mundësi në internet pa pasur nevojë të kufizohen nga strategjitë kufizuese të ndërmjetësimit.

Radikalizimi mund të burojë nga:

- Qëllime politike (për shembull, ndryshimi i formës së qeverisjes, si heqja e sistemit demokratik me zgjedhjet që kemi tani dhe vendosja e një diktature).
- Qëllime shoqërore (për shembull, kur anëtarët e klubeve të tifozëve të sportit përpiqen të bëjnë një ndryshim ose të arrijnë një qëllim - të bindin sportdashësit e klubeve të tjera të mbështesin klubin e tyre).
- Qëllime fetare (për shembull, kur anëtarët e një feje të veçantë dëshirojnë të imponojnë një ndryshim që do ta bëjë fenë e tyre dominuese ose ekskluzive).

Procesi i indoktrinimit në internet shpesh ndodh përmes diskutimeve (bisedave), bindjes, ndikimit, afeksionit ose mësimdhënies të organizuara në grupe të mbyllura ose të izoluara, forumeve, dhomave të shpëtimit. 'Të bashkuar nga revistat në internet, blogjet, shërbimet dhe dhomat e bisedave, pjesëmarrësit hyjnë në forume ku ideologjia ekstremiste bëhet vetë-përforcuese' (Schaan dhe Phillips, 2011, f. 24).

Procesi i radikalizimit të dhunshëm në internet përmes hapësirës kibernetike në vendin tonë, si kudo tjetër, ndryshon. Duke qenë se ky proces është i përshtatur nga personi (synimi), ai mund të ndjekë modele dhe dinamike specifike. Gjatë procesit të rekrutimit ata që radikalizohen përpiqen të tërheqin dhe përfundimisht të izolojnë një individ (ose një grup), në mënyrë që personi të mund të bashkohet, duke përdorur ankesat politike dhe/ose socio-ekonomike si një hap për mobilizimin drejt një ndryshimi duke përdorur atë se çfarë do të thotë dhuna.

Radikalizimi i dhunshëm në internet zakonisht fillon me një përzgjedhje që mund të synohet dhe organizohet, ose mund të jetë spontane, d.m.th. vetë-përzgjedhje kur dikush zgjidhet përmes sjelljes së tij ose të saj⁵.

Përdorimi i teknologjive moderne dhe sjelljes sociale të mësuar (d.m.th. të qenit komod për të përdorur teknologjitë dhe aplikacionet moderne të komunikimit si komunikim konvencional në botën fizike).⁶ Për këtë qëllim (përzgjedhja), disa nga grupet dhe individët e organizuar mirë, me qëllim të keq kanë hartuar një metodologji të profilizimit. Duke skanuar aktivitetet në internet, duke mbledhur dhe përpunuar të dhëna (duke analizuar sjelljen e synuar) këto grupe ose individë inicojnë procesin e përzgjedhjes. Ekzistojnë disa mënyra përmes të cilave grupe të dëmshme dhe individë mund të mbledhin të dhëna personale nga të rinjtë në internet, përfshirë:

- Profilin personal në çdo platformë (Facebook, Twitter, Instagram, YouTube) për qëllime komunikimi dhe video. Ata mund të ekzaminojnë zakonet personale, sjelljet e blerjes, dëshirat, hobet dhe ndikuesit, vendet dhe faqet e interesit të personit të synuar dhe të identifikojnë dobësitë e tij/saj. Qasja për të mbledhur këtë sasi të dhënash mund të jetë ose duke shfrytëzuar mbrojtjen e dobët të profilit në internet të njerëzve ose aq e thjeshtë sa dërgimi i një kërkesë të rastësishme miqësie në Facebook. Metoda të ndryshme për të identifikuar individë të prekshëm nga idetë ekstremiste mund të përfshijnë thurje (hashtags) të caktuar në një postim të mediave sociale, etj.
- Mbledhja e informacionit përmes faqeve të internetit dhe forumeve për biseda. Shumë shpesh njerëzit me qëllime dashakeqe kanë faqe të organizuara mirë që janë tërheqëse dhe të mbushura me përmbajtje të dedikuara për individë dhe grupe të caktuara që ka gjasa të shfletojnë përmbajtjen⁷. Informacioni në këto faqe në internet mund të jetë i vërtetë, pjesërisht i vërtetë dhe plotësisht i rremë.⁸ Faqet e internetit

⁵ Metodi Haxhi-Janev, Mitko Bogdanoski, Dimitar Bogatinov (2020) *"Drejt të rinjve të sigurtë në internet: Përqaftimi i konceptit të medias dhe shkrim-leximit të informacionit"*, KAS

⁶ Shikoni për shembull: Postmes Tom & Brunsting Suzanne, (2002), "Veprimi kolektiv në epokën e internetit: Komunikimi masiv dhe mobilizimi në internet", Social Science Computer Review, 20, 290-301, në dispozicion në:
<https://journals.sagepub.com/doi/10.1177/089443930202000306>

⁷ 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.

⁸ Disa hulumtime të pavarura e konfirmojnë këtë, shih për shembull: Brachman Jarret dhe Levine Alex, (Prill 13, 2011), *"The World of Holy Warcraft"*, Politika e Jashtme, e disponueshme në: <http://foreignpolicy.com/2011/04/13/the-world-of-holy-warcraft/>;

ose forumet e bisedave mund të jenë të lidhura ose jo me përmbajtjen që është qëllimi përfundimtar. Këto faqe shpesh shfaqin përmbajtje që përgatitet paraprakisht për të testuar viktimën e mundshme.⁹ Mbledhësit dinë si të masin reagimet individuale ndaj përmbajtjes së caktuar dhe të formojnë një strategji për t'iu qasur objektivit të identifikuar bazuar në atë.

- Mbledhja e informacionit duke e parë përmbajtjen e videos. Ashtu si me teknikat e tjera për monitorimin e sjelljes, rekrutuesit në internet mund të shfrytëzojnë historinë e shfletimit të një personi për të mbledhur të dhëna. Shumica e platformave kanë algoritme - programe të përshtatshme që zgjedhin se çfarë po shihni në to. Në disa platforma, videot e postuara kanë një listë të pamjeve individuale, me qasje në profilet e shikuesve. Dikush mund të dallohet shumë lehtë nëse ata shikojnë video që kanë përmbajtje që synon të joshë përcjellësit e rinj në një botëkuptim të veçantë ideologjik që kërkon dhunë. Edhe pse janë të synuara mirë, disa tipare të aplikacioneve sociale shfrytëzohen nga organizatat terroriste siç janë udhëzimet e YouTube se si të krijoni një video bazuar në profilin/zakonet e shikuesve ose ndjekësve të dëshiruar. Është shumë e lehtë që rekrutuesit të keqpërdorin këtë metodë për qëllimet e tyre.¹⁰
- Lojërat. Lojërat janë një mënyrë tjetër që mentorët në internet që janë radikalë dhe kërkojnë ndjekës të rinj, të mund të kenë qasje në informacionin personal. Lojërat moderne video, dhe aplikacionet e lojërave, lejojnë komunikimin në një dhomë bisede të krijuar posaçërisht nga një lojtar në tjetrin dhe si të tilla krijojnë mundësinë e përsosur për grabitqarët. Për shembull, fshehja pas një karakteri të lojës për të gjeneruar një diskutim brenda formës së gjuhës së urrejtjes, e cila nga ana tjetër mund të përdoret lehtësisht si një formë e agresionit kundër grupeve/individëve nga bota fizike.¹¹ Sipas disa statistikave, të rinjtë në vendin tonë preferojnë të luajnë në internet,

ose shih: Behr Ines Von, Reding Anaïs, Edwards Charlie & Gribbon Luke, (2013); ose: Sageman Martin, (2008), "Leaderless Jihad", University of Pennsylvania Press

⁹ Busher Joel (2015), "What part do social networks play in radicalisation?", Kërkimi i radikalizimit, i disponueshëm në: <http://www.radicalisationresearch.org/debate/busher-social-networks/>

¹⁰ Shih më shumë në YouTube Creator Academy, e qasshme në:

<https://creatoracademy.youtube.com/page/lesson/discoverability-analytics>

¹¹ 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, në dispozicion në:

<https://www.semanticscholar.org/paper/Skinhead-Super-Mario-Brothers%3A-An-Examination-of-on-Selepak/581e60a66b63bd58853d9cffb9304fb81f25314e>

dhe 38% përdorin internetin për të luajtur dhe shkarkuar lojëra, që është shumë mbi mesataren evropiane prej 34%.¹²

Vlerësimi bazë i Studimit të CRPM "Passage4prevent: përdorimi i arsimit për të parandaluar radikalizimin onlajn të të rinjve" zbulon se mbi gjysma e nxënësve të shkollave të mesme të anketuara, shumë shpesh kanë qasje në përmbajtjen e trolling, ngacmimeve dhe ofendimeve në internet (52.7%), e ndjekur nga përmbajtje të dhunshme me humor të portretizuar (47.7%), ose përmbajtje që tregojn sulm fizik, nxitje dhe rrahje (39.9%) dhe gjuhë urrejtjeje që inkurajon drejtpërdrejt njerëzit të sillen me dhunë ose të kryejnë një akt dhune (39.2%). Interesante, mbi 20% e nxënësve të anketuar kanë konfirmuar se kjo lloj përmbajtje e dhunshme në internet ndahet nga të paktën gjysma e miqve të tyre. Kjo sugjeron përhapjen e gjerë të përmbajtjes së dhunshme në internet dhe nivelin e lartë të ekspozimit të të rinjve ndaj dhunës. Sidoqoftë, nëse ekziston rreziku i përdorimit të kësaj përmbajtje për të radikalizuar dhe pranuar ide ekstremiste të dhunshme, duhet të hulumtohet më tej.

Pasi grabitqarët të kenë gjetur një shënjestër që përdor çdo komunikim të mediave sociale (Facebook, Twitter, Instagram, Snapchat, YouTube, etj.) në internet, ata kalojnë në fazën tjetër të rekrutimit: afrimi dhe izolimi. Komunikimi fillestar zakonisht është në mbështetje të ankesave të viktimës për të fituar besimin e tyre.¹³ Kjo do të thotë se "personi" dhe "grupi" mund të krijojnë marrëdhënie të veçanta në internet për shkak të interesave, shprehjeve, përvojave, pikëpamjeve, mendimeve dhe qëndrimeve të ngjashme. Shumica e këtyre ngjashmërive të pretenduara janë të paracaktuara dhe të përshtatura bazuar në procesin e profilizimit. Më shpesh, gjatë kësaj periudhe përfaqësues të mirëorganizuar të grupeve dashakeqe paraqiten si anëtarë që ndajnë pikëpamje të ngjashme me viktimën, dhe kështu së fundmi investojnë në krijimin e besimit në "dhomë" (dhomën e bisedave). Qëllimi përfundimtar në këtë fazë është krijimi i një lidhjeje. Për këtë qëllim, ata krijojnë dhoma të mbyllura të bisedave. Këtu fillon izolimi.

Për të avancuar dhe krijuar izolim të mëtejshëm, viktimat mund të marrë një ofertë ekskluzive. Një shembull mund të jetë një propozim për privilegje të caktuara, d.m.th. për t'u bërë anëtar i "atyre të veçantë".¹⁴ Një metodë tjetër

¹² Ироп Петровски, (Qershor 29, 2018), „Младите и интернетот“, Капитал

¹³ Weimann Gabriel, (2015)

¹⁴ Weimann, Gabriel, (2010), "Terror on Facebook, Twitter, and Youtube", Brown Journal of World Affairs, 16(2), 45-54, në dispozicion në: <http://bjwa.brown.edu/16-2/terror-on-facebook-twitter-and-youtube/>

për të izoluar objektivin mund të jetë hyrja me rekomandim në grupe të zgjedhura ose të veçanta ku ndodhin të gjitha "temat e nxehta".



Diskutimet e përgatitura paraprakisht me qëllim mund të përfshijnë zakonisht tema të tilla si trazira, ndryshimi i sistemit dhe gjuha e urrejtjes kundër atyre që janë të ndryshëm. Në përgjithësi, grupet e mbyllura kanë rregulla të bazuara në parimet "vetëm për anëtarët". Qëllimi në këtë fazë është krijimi i ndjenjës së përkatësisë dhe që viktimat të ndihet e barabartë me të tjerët. Besimi i fituar mund të përfshijë edhe kompensimin. Një personi (viktimë e radikalizimit të dhunshëm në internet) mund t'i kërkohej për një shërbim (për të bërë diçka) për të cilin ai/ajo do të shpërblehet. Pasi të fitohet besimi, fillon procesi i ndërtimit të një identiteti të përbashkët (indoktrinimi).¹⁵

Vlerësimi Bazë i Studimit të CRPM *"Passage4prevent: përdorimi i arsimit për të parandaluar radikalizimin onlajn të të rinjve"* zbulon se 44% e të anketuarve marrin përmbajtje të dhunshme përmes mesazheve personale (inbox) ose në dhomat e bisedave. Ndërsa të tjerët, 37% e nxënësve të shkollës së mesme, të anketuarit në sondazhin e CRPM thanë se këto lloje të përmbajtjes së dhunshme ndahen gjithashtu përmes grupeve të krijuara për shpërndarje. Kjo sugjeron që infrastruktura dhe modeli i sjelljes që përdoret në radikalizimin në internet (izolimi dhe indoktrinimi) praktikohet dhe normalizohet midis një numri të madh të nxënësve të shkollave të mesme që paraqet një rrezik për radikalizimin e mundshëm në internet.

¹⁵ Disa e kanë quajtur këtë proces "shkrirja e identitetit", shih: Swann William Jr. & Buhrmester D, Michael (2015), "Identity Fusion", Psychological Science, Vol. 24(1) 52–57, në dispozicion në: <https://labs.la.utexas.edu/swann/files/2016/03/52-57.pdf>

Gjatë fazës së indoktrinimit, formulime dhe fraza të caktuara dominojnë në dhomat e biseduara të izoluara për të inkurajuar një pozicion të përgjithshëm mbi çështje konkrete. Nuk ka asnjë rregull për sa kohë kalon nga procesi i përzgjedhjes në indoktrinim. Mund të jetë një proces i gjatë, por gjithashtu mund të ndodhë shumë shpejt. Ky proces bëhet përmes manipulimit - besimi se diçka që duhet ndryshuar duhet të bëhet, edhe nëse përfshin përdorimin e dhunës. Manipulimi synon të prodhojë shtrembërim dhe abuzim me besimet, ideologjitë politike dhe dallimet etnike dhe kulturore (tërheqjen e pikëpamjeve të thjeshta globale që ndajnë botën në "ne kundrejt tyre"), duke nxitur kështu viktimat të kërkojnë përgjigje.¹⁶

Bazuar në një ekzaminim të 150 artikujve, nga të cilët vetëm 18 ishin studime të nxjerra në mënyrë empirike, RAND ka identifikuar shtëpinë e prodhimit mediatik të Al Kaeda-s, Fondacioni As-Sahab për Publikimin e Mediave Islamike dhe faqet e tyre të internetit si burim i tillë. Vetë radikalizimi mund të ndodhë gjithashtu kur një viktimë e rastësishme lexon literaturë, forume dhe blogje nga burime të dyshimta ose transmeton video, regjistrime audio, ose këngë me përmbajtje që ka për qëllim të radikalizojë me dhunë.

Fraza si "neve", "ne", "së bashku" dhe "tonë" përdoren për të rritur përkatësinë, për të kompensuar fatkeqësitë dhe tragjeditë dhe për të inkurajuar sjelljen e përshtatur përmes besnikërisë së shkaktuar, dhe kërkimin për "tronditje dhe aventurë" dhe "fuqi dhe kontroll" - duke zëvendësuar botën reale me botën virtuale¹⁷. Bazuar në profilizimin në grupin e izoluar gjatë procesit të indoktrinimit, objektivat mund të shprehen, të ndihen rehat emocionalisht dhe të mbrojtura. Këto grupe krijojnë një rreth besimi dhe kur viktimat ndihet i sigurt, ai individ është i gatshëm të implantohet me sjelljen që më parë perceptohej si e gabuar, e ndaluar ose e çuditshme¹⁸. Përdorimi i dhunës shpesh bëhet justifikimi moral ndaj të gjitha shanseve që e kanë vendosur viktimën në polin e kundërt të spektrit të polarizuar në shoqëri.

¹⁶ Ibid.

¹⁷ Në hulumtimin e Iniciativës Atlantike në vitin 2017, e ashtuquajtura prekje njerëzore identifikohet gjithmonë si fillimi i radikalizimit, në botimin e Azinovic, V (ed) (2017). "Between Salvation and Terror: Radicalisation and the Foreign Fighter Phenomenon in the Western Balkans. The Atlantic Initiative, fq. 17, në dispozicion: http://www.atlantskainicijativa.org/bos/images/BETWEEN_SALVATION_AND_TERROR/BetweenSalvationAndTerror.pdf

¹⁸ Në Manualin e UNESCO-s këta faktorë veçohen si faktorë tërheqës. Shih më shumë në UNESCO, (2017), op.cit.

Praktika tregon se i gjithë procesi i përshkruar më sipër mund të ndodhë përmes "vetë-radikalizimit".¹⁹ Siç u përmend më parë, faqet e parapërgatitura manipuluese mund të gjenden në internet dhe të cilat përdorin tekste, video dhe muzikë të shkruara për të shtrembëruar faktet dhe për të ushtruar ndikim drejt radikalizimit të dhunshëm ose vetëradikalizimit të dhunshëm.

Rishikimi i literaturës ka identifikuar pesë rolet e mëposhtme që interneti ka në promovimin e radikalizimit: (i) interneti krijon më shumë mundësi për t'u radikalizuar²⁰; (ii) interneti vepron si një 'dhomë jehone'²¹; (iii) interneti përshpejton procesin e radikalizimit²²; (iv) interneti lejon radikalizimin të ndodhë pa kontakt fizik²³; (v) interneti rrit mundësitë për vetëradikalizim²⁴. Brezi i ri, është veçanërisht i prekur ndaj radikalizimit në internet pasi ata pranojnë media onlajn shumë më natyrshëm si një pjesë e jetës së tyre dhe marrëdhëniet e tyre shoqërore se sa brezat e vjetër²⁵. Kjo do të thotë që rëndësia e komunikimit ballë për ballë është në rënie dhe kontaktet në internet hasen me shumë besim, duke bërë që ndërhyrjet e politikave drejt rritjes së sigurisë në internet të jenë përparësi e çdo qeverie.

¹⁹ Më shumë rreth kësaj mund të gjenden në: Sageman Martin (2008), "Leaderless Jihad: Terror Networks in the Twenty-First Century", Philadelphia: University of Pennsylvania Press

²⁰ Pantucci 2011; Briggs and Strugnell 2009; Homeland Security Institute 2009; Weimann 2006; Precht 2008 i cili zbuloi se ekziston një korrelacion midis faqeve të xhihadit dhe propagandës në internet dhe radikalizimit të shpejtë në një studim empirik të 242 xhihadistëve evropianë nga 2001-2006.

²¹ Interneti është përshkruar si një 'dhomë jehonë' (Ramakrishna, 2010; Saddiq, 2010; Stevens and Neumann, 2009) ose një 'aktivitet i përforcimit mendor' (Silber and Bhatt, 2007) që siguron anonimitet të supozuar (Weimann, 2006) dhe një shkallë të mbrojtjes dhe sigurisë nga zbulimi (Gray and Head, 2009), si dhe siguron pranim: informacioni është i jo-censuruar dhe jo-hierarkik (Bartlett, 2011)

²² Schmidle (2009) tregon rolin e dhomave të bisedës në veçanti në këtë efekt përshpejtimi, pasi ekstremistët mund të shkëmbejnë me individë me të njëjtin mendim 24/7, pavarësisht nga kufijtë

²³ 'Individët kanë komoditetin për të hyrë në përmbajtjen radikale nga hapësira e tyre personale në vend që të kalojnë nëpër shqetësimet e 20 tubimeve radikale fetare me tubime fizike (Yeap and Park, 2010, p. 2)

²⁴ Sipas RAND (2013) 'Radikalizimi në epokën digjitale' "Ajo që e dallon vetë-radikalizimin nga radikalizimi përmes internetit është se ajo zhvillohet në izolim, dhe nënkupton një proces ku asnjë kontakt nuk bëhet me terroristë të tjerë ose ekstremistë, qoftë personalisht apo praktikisht".

²⁵ KAS (2013) "Online-Radicalisation: Myth or Reality?", në dispozicion: https://www.kas.de/c/document_library/get_file?uuid=baca4877-ac6c-4df4-ae77-28b4ba2aafac&groupId=252038

Përgjigja e politikës ndaj radikalizimit në internet

Sfida për qeveritë dhe të gjithë aktorët e interesuar është të kuptojnë gamën e faktorëve në të cilët media sociale mund të luajë një rol në këtë mënyrë që përgjigjet të mos gabohen ose të bazohen në supozime të pambështetura²⁶. Mbi këtë bazë, mund të jetë e mundur të identifikohen hapat e duhur për të kundërshtuar veprimtarinë radikalizuese në internet dhe për të siguruar kornizat e duhura ligjore, institucionale, administrative dhe arsimore për t'iu përgjigjur kërcënimit, në përputhje të plotë me ligjin ndërkombëtar të të drejtave të njeriut. Hapat duhet të sigurojnë që liria e shprehjes dhe privatësia janë të lira nga ndërhyrjet arbitrare, të paligjshme ose disproporcionale dhe janë në gjendje të ruajnë karakteristikat e internetit duke qenë i hapur, gjithëpërfshirës dhe duke kontribuar në zhvillimin e qëndrueshëm dhe prosperitetin e shoqërisë moderne²⁷.

Përkundër situatës së brishtë të vazhdueshme, puna për CVE në vend është e kufizuar, dhe për radikalizimin onlajn të të rinjve edhe më shumë. Analytica²⁸ i studioi drejtuesit e ekstremizmit duke përfshirë faktorë të ngjashëm me ata që e nxisin ekstremizmin global. Bashkësia Islame e Maqedonisë nisi trajnimin e ekstremizmit të dhunshëm (CVE) për hoxhallarët për të inkurajuar komunitetin për të gjetur një alternativë ndaj përqafimit të dhunës. Fondacioni Berghof filloi me kërkimin bashkëpunues dhe iniciativën e dialogut duke eksploruar pse disa komunitete preken veçanërisht, ndërsa komunitetet e tjera mund të tregojnë një rezistencë më të madhe ndaj radikalizimit. Qendra për Kërkime dhe Hartim të Politikave zhvilloi kërkime mbi perceptimet e mësuesve dhe punëtorëve të vijës së parë mbi radikalizimin dhe ekstremizmin e dhunshëm, dhe kapacitetet e ndërtuara përmes zhvillimit të udhëzimeve dhe mjeteve (listave të kontrollit dhe protokolleve) dhe punëtorive trajnuese për zbulimin e hershëm të radikalizimit. Gratë pa Kufij, nxiti projektin e shkollës së nënës që synon të rrisë ndërgjegjësimin për t'iu kundërvënë radikalizmit dhe të rrisë kompetencat dhe aftësitë e nënave të vendit tonë për t'u marrë me

²⁶ Dan Shefet (2016) Policy options and regulatory mechanisms for managing radicalization on the Internet, UNESCO

²⁷ UN (2015) Plan of Action to Prevent Violent Extremism, në dispozicion: <https://undocs.org/A/70/674>

²⁸ Analytica, 2016 "Assessment of Macedonia's Efforts in Countering Violent Extremism"

fenomenin e radikalizimit, në marrëdhëniet e tyre me fëmijët. OSBE-ja ka trajnuar mësues që të bëhen trajnerë për çështje që lidhen me radikalizimin dhe ekstremizmin e dhunshëm. IOM ka punuar në nivelin e komunitetit duke siguruar trajnim për të menduarit IC për të rinjtë. CRPM ka zhvilluar një kurrikulë trajnimi për nxënësit e shkollave të mesme për të rritur njohuritë dhe aftësitë e tyre për përdorimin e sigurt të internetit në një përpjekje për të ndërtuar qëndrueshmëri ndaj radikalizimit në internet, si dhe ka zhvilluar një Manual për sigurinë kibernetike në shkolla për të rritur qëndrueshmërinë ndaj radikalizimit në internet.

Sa i përket kornizës së politikave, Strategjia për luftimin dhe parandalimin e ekstremizmit të dhunshëm rregullon qëllimet përkatëse siç është qëllimi Strategjik 1.1. Kapacitetet e forcuara institucionale; Qëllimi strategjik 1.4: Parandalimi i radikalizimit përmes internetit dhe Qëllimi Strategjik 3.1: Vendosja e masave për zbulimin e hershëm të radikalizimit kombëtar. Strategjia është në përputhje me Strategjinë Globale të Kundër Terrorizmit të Kombeve të Bashkuara që midis përparësive të saj të veprimit parashikon "domosdoshmërinë për të mbështetur" Edukimin, zhvillimin e aftësive dhe lehtësimin e punësimit "si një mjet për të nxitur respektin për diversitetin njerëzor dhe përgatitjen e të rinjve për të hyrë në vend pune"²⁹. Në mënyrë të ngjashme, ai është i efektshëm me Strategjinë e BE-së Kundër Terrorizmit dhe Manifesti RAN për Arsimin-Fuqizimin e Edukatorëve dhe Shkollave.³⁰

Më konkretisht Strategjia e Sigurisë Kibernetike me të drejtë tregon se hapësira kibernetike mund të përdoret për terrorizëm dhe e identifikon atë si një kërcënim të mundshëm të sigurisë kombëtare, si pjesë e qasjes më të gjerë ndaj parimeve të sigurisë kibernetike³¹. Sidoqoftë, nuk parashikon qëllime dhe as aktivitete që synojnë posaçërisht të rinjtë, aftësinë ose qëndrueshmërinë e tyre ndaj ideve radikale ose terrorizmit të lehtësuar në internet. Sfidë për të adresuar radikalizimin në internet i bën jehonë sfidave

²⁹ Strategjia Globale Kundër Terrorizmit e Kombeve të Bashkuara (A/RES/60/288), miratuar nga Asambleja e Përgjithshme e KB më 8 shtator 2006, është një instrument unik global për të rritur përpjekjet kombëtare, rajonale dhe ndërkombëtare për të luftuar terrorizmin. Për më shumë informacion vizitoni:

<https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy>

³⁰ RAN Manifesti për arsimin i disponueshëm në: 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

³¹ Qeveria e Republikës së Maqedonisë së Veriut, Republika e Maqedonisë së Veriut: Strategjia Kombëtare e Sigurisë Kibernetike 2018 - 2022, fq.12 në dispozicion në: https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf

të përgjithshme që lidhen me kapacitetet institucionale për qeverisjen elektronike. Për shembull, një vlerësim i pavarur i kapaciteteve të sigurisë kibernetike të vendit, i drejtuar nga Banka Botërore dhe Qendra Globale e Sigurisë Kibernetike në vitin 2018, pohoi se *"Nuk ishte e mundur të sigurohej një fotografi e qartë në lidhje me menaxhimin e krizës ..."* gjatë rrjedhës së kërcënimeve kibernetike.³²

Plani strategjik për arsimin 2020-2022³³ parashikon qëllimin strategjik 2.2 Arsimi i mesëm cilësor dhe gjithëpërfshirës që është në përputhje me dokumentin strategjik 'Reforma në arsim dhe investimet në inovacione dhe teknologjinë e shoqërisë informatike', por i mungon përparësia, aktivitetet dhe treguesit kryesorë të performancës në lidhje me rritjen e qëndrueshmërisë së nxënësve të shkollave të mesme për radikalizimin në internet, dhe as përmend sigurinë në internet të nxënësve.

Koncepti për mësimin në distancë³⁴ përcakton që shumica e sistemeve arsimore evropiane kanë përfshirë kompetencat digjitale si një temë horizontale, por në shumë vende të Evropës Lindore çështjet e sigurisë në internet dhe ndërtimin e rezistencës së të rinjve trajtohen me një qasje më holistike si pjesë e një strategjie gjithëpërfshirëse, ndërsa në Evropën Perëndimore, Qendrore dhe atë të Veriut këto çështje trajtohen me një strategji të veçantë. Në Maqedoni, kompetencat digjitale fitohen përmes dy lëndëve, një e detyrueshme dhe një me zgjedhje, por çështjet e sigurisë në internet janë të mbuluara thjesht me programin mësimor.³⁵

Në klasën e pestë sistemi arsimor i Maqedonisë për arsimin fillor parasheh kursin Punë me kompjuter dhe bazat në programimin kompjuterik i cili sipas programit mësimor³⁶ përfshin vetëm një përmbajtje në lidhje me sigurinë në internet: diskutimi për komunikimin në internet dhe çështjet e sigurisë në lidhje me komunikimin në internet.

³² Banka Botërore & Qendra Globale e Sigurisë Kibernetike, (2018), "Cybersecurity Capacity Review, Former Yugoslav Republic of Macedonia (FYR Macedonia)", Wordl Bank, fq.9 e disponueshme në: https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

³³ MASH (2019) Plani strategjik 2020-2022, i disponueshëm në internet: <https://mon.gov.mk/stored/document/Strateski%20plan%20%202020-2022.pdf>

³⁴ MASH (2020) Koncepti për zhvillimin e sistemit të mësimin në distancë në shkollat fillore dhe të mesme

<https://mon.gov.mk/content/?id=3262>

³⁵ https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatika-I_SSO-trigodishno-mkd.pdf

³⁶ https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Rabota_so_kompjuter_i_osnovi_na_programiranjeto-V_odd-2020.pdf

Në klasën e gjashtë, sistemi arsimor i Maqedonisë për arsim fillor parasheh kursin *Informatik*, i cili sipas programit mësimor³⁷ ka shtatë qëllime nga të cilat katër kanë të bëjnë me shkencën kompjuterike, njëra ka të bëjë me teknologjinë e informacionit dhe dy janë duke u përqëndruar në kompetencat digjitale. Një nga objektivat e kompetencave digjitale që është më e rëndësishme për ndërtimin e rezistencës në internet është përdorimi i teknologjisë në mënyrë etike dhe me përgjegjësi dhe në mënyrë të sigurt për të mbajtur informacionin personal. Në këtë drejtim, parashikimet e kurrikulës që rregullat e sigurisë do të përcaktohen nga nxënësit për klasën ku zhvillohet klasa e Informatikës dhe diskutimi me nxënësit, do të nxitet për të përcaktuar etikën në përdorimin e kompjuterit dhe keqpërdorimin e mundshëm. Sa i përket sigurisë në internet, gjithashtu është diskutuar një diskutim mbi çështjet e sigurisë në komunikimin në internet në semestrin e dytë. Sidoqoftë, vlerësimi i informacionit, të dhënave dhe përmbajtjes digjitale dhe rreziku i tyre për radikalizim në internet nuk është parashikuar.



Në klasën e shtatë kursi *Informatik*³⁸ është një kurs i detyrueshëm që përfshin 5 klasa për jetesë në internet që në mënyrë indirekte trajtojnë gjithashtu sigurinë në internet. Në mënyrë indirekte, pasi kurrikula nuk përfshin përmbajtje mbi sigurinë dhe kompetencat për vlerësimin e përmbajtjes digjitale, por ndërton aftësi për krijimin e faqeve në internet, blogje etj.

³⁷ https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Informatika-VI_odd-2020.pdf

³⁸ https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Informatika-VII_odd-2020.pdf

Rekomandohet që të përdoren burime të temave të jetesës në internet që ofrojnë rekomandime për përdorimin e sigurt të internetit. si materiale mësimore të tilla si faqet e internetit të: <http://bezbednonainternet.org.mk>, www.dzlp.mk, dhe www.iSafe.org.

Në klasën e tetë dhe të nëntë informatika nuk ofrohet si kurs i detyrueshëm ose me zgjedhje në sistemin arsimor fillor të Maqedonisë.

Në arsimin e mesëm nxënësit në arsimin e mesëm të përgjithshëm, i ashtuquajtur gjimnaz, kanë *Informatikë* si një kurs të detyrueshëm në vitin e parë i cili i njeh ata me harduerin, softuerin dhe hyrjen themelore në programim³⁹, por asnjë përmbajtje në kurrikulë që lidhet me sigurinë në internet dhe kompetencat digjitale që mund të ulin ndjeshmërinë ndaj radikalizimit në internet. Në vitin e dytë kjo lëndë ofrohet si lëndë zgjedhore së bashku me teknologjinë e informacionit si lëndë⁴⁰, ndërsa në të tretin⁴¹ dhe vitin e katërt⁴² pasi ofrohet një programim i detyrueshëm. Asnjë nga programet mësimore nuk përfshin kompetencat digjitale dhe në veçanti çështjet që lidhen me sigurinë si mbrojtja e pajisjeve, mbrojtja e të dhënave personale dhe privatësisë, mbrojtja e shëndetit dhe mirëqenies siç kërkohet nga Korniza e Kompetencave Digjitale për Qytetarët e Komisionit Evropian⁴³.

Korniza e Kompetencave Digjitale është miratuar në vitin 2016 dhe azhurnuar në vitin 2018, parashikon 5 fusha kryesore të matura dhe monitoruara nga Bashkimi Evropian: (i) shkrim-leximi digjital; (ii) komunikimi dhe bashkëpunimi; (iii) zhvillimi i përmbajtjes digjitale; (iv) siguria; dhe (v) zgjidhja e problemit. Nga analiza e kurrikulës së paraqitur më lart, duket se arsimi fillor i Maqedonisë është më i drejtuar drejt ndërtimit të aftësive dhe rritjes së njohurive mbi shkrim-leximin digjital, si dhe komunikimit dhe bashkëpunimit; ndërsa ai i mesëm për zhvillimin e përmbajtjes digjitale dhe në një farë mase zgjidhjen e problemeve, por ajo që plotësisht mungon në të dy nivelet e arsimit është përqendrimi te siguria.

³⁹ https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatika-I_SSO4-mkd.pdf

⁴⁰ https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatichka_tehnologija-II_GO-mkd.pdf

⁴¹ https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Programski_jazici-III_GO-PMA-mkd.pdf

⁴² https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Programski_jazici-IV_GO-mkd.pdf

⁴³ 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>

Duke e marrë parasysh që rezultatet e Vlerësimit Bazë të Studimit CRPM "*Passage4prevent: Përdorimi i arsimit për të parandaluar radikalizimin në internet të të rinjve*" tregon se rreth tridhjetë përqind e nxënësve të shkollave të mesme në komunat e studiuara po ndajnë informacione personale me të huajt mbi komunikimin në internet⁴⁴, të tilla si emri, moshë, adresat e postës elektronike, shkolla, fotot personale etj. dhe që një pjesë e madhe e tyre thanë që rrallë ose kurrë nuk kontrollojnë besueshmërinë e informacionit në internet (40,7%), duke i bërë kështu të prekur ndaj lajmeve të rreme, dezinformimit, ideve radikale në internet. Kjo e bën përqendrimin në sigurinë në internet një përparësi që duhet të trajtohet si me ndryshimet legislative/kurrikulare, ndërtimin e kapaciteteve dhe llojin e përgjigjeve të politikës shkollore. Kuadri **DigiComp2.0** mund të shërbejë si një udhërrëfyes për arritjen e këtij objekti.

Në këtë proces nxënësit dhe familjet e tyre, si dhe e gjithë shoqëria janë përfitues, ndërsa shkollat dhe mësuesit/edukatorët janë palët e interesuara që veprojnë si agentë. Në veçanti mësuesit duhet të jenë në shënjestër të drejtpërdrejtë pasi Vlerësimi Bazë i Studimit CRPM "*Passage4prevent: Përdorimi i arsimit për të parandaluar radikalizimin në internet të të rinjve*" tregon se kur nxënësit ndihen të kërcënuar ndërsa janë në internet, 61% e tyre do të flasin me prindërit/kujdestarët e tyre, 20% zgjedhin për të folur me një mik, ndërsa 16% do të raportojnë kërcënimin në polici, dhe vetëm 1% thanë se do të flisnin me mësuesit/profesorët nëse ndihen të kërcënuar në internet. Kjo sugjeron mungesë besimi te mësuesit, ose roli i tyre në ndërtimin e qëndrueshmërisë dhe kompetencës digjitale nuk është i dukshëm dhe i njohur nga nxënësit. Kjo mund të jetë për shkak të mungesës së kompetencave, ose mungesës së politikave shkollore për garantimin e sigurisë në internet. Për këtë qëllim nxënësit e shkollës së mesme që morën pjesë në sondazhin e CRPM mendojnë se prindërit e tyre kanë më shumë njohuri (79% e të anketuarve), krahasuar me mësuesit për të cilët 63.6% e të anketuarve thanë se kanë disi njohuri në lidhje me internetin dhe aftësitë e tij. Ka një përqindje mjaft të lartë të nxënësve (16.7%) të cilët mendojnë se mësuesve të tyre u mungon njohuria. Prandaj, rritja e kompetencave të mësuesve duhet të jetë një pjesë e rëndësishme e politikës gjithëpërfshirëse për qëndrueshmëri të shtuar për radikalizimin në internet. Kuadri Evropian

⁴⁴ Sondazhi tregon, 32.6% e të anketuarve thanë se e kanë ndarë emrin e tyre me dikë që kanë takuar vetëm në internet, 31.8% kanë ndarë moshën e tyre, 29.5% kanë ndarë informacione për shkollën në të cilën studiojnë, ndërsa 23.8% kanë shpërndarë fotot e tyre. 21.1% e nxënësve të shkollave të mesme kanë shkëmbyer informacion me dikë që kanë takuar vetëm në internet për vendin ku ata shkojnë.

për Kompetencat Digjitale të edukatorëve/mësuesve⁴⁵ mund të shërbejë si një dokument i politikës udhëzuese për atë objektiv. Korniza **DigiEduComp** përfshin gjashtë fusha ku duhet të ndërtohen kompetencat e mësuesit: (i) angazhimi profesional; (ii) burimet digjitale; (iii) edukimi dhe të mësuarit; (iv) vlerësimi; (v) mbështetja e nxënësve dhe (vi) përmirësimi i kompetencave digjitale të nxënësve në drejtim të informacionit dhe edukimit mediatik, komunikimit, zhvillimit të përmbajtjes, përdorimit të përgjegjshëm të internetit dhe zgjidhjes së problemeve.

Për më tepër, përveç një shkolle në Shkup, 41 shkollat e mbetura në projekt nuk kishin politikë digjitale të sigurisë, dhe as ndonjë masë të zbatuar drejt këtij qëllimi. Lidhur me faktin nëse duhet të ketë një politikë/udhëzim për përdorimin e telefonave inteligjentë/pajisjeve dhe internetit në shkollë, të rënë dakord midis mësuesve, nxënësve dhe prindërve/kujdestarëve që do të përfshijë udhëzime për aspekte të caktuara të përdorimit, 73% e nxënësve të shkollës së mesme/të anketuarit në Vlerësimin Bazë të Studimit të CRPM *“Passage4Prevent: Përdorimi i arsimit për të parandaluar radikalizimin në internet të të rinjve”* do të aprovonin një udhëzues të tillë në përgjithësi. Sipas aspekteve specifike që duhet të mbulohen nga udhëzimet, mbështetja është: a) mbrojtja e përmbajtjes në internet (78.8%), b) mosndarja e informacionit dhe të dhënave personale (70.3%), c) sjellja e internetit në lidhje me mbrojtjen nga dhuna kibernetike (78.8%), d) kontrollimi i informacionit (66.9%). Prandaj, Ministria e Arsimit duhet të ndërmarrë një iniciativë për zhvillimin dhe miratimin e politikave shkollore për sigurinë në internet për të ulur ndjeshmërinë ndaj radikalizimit në internet. Për këtë qëllim, Korniza e Organizatave Arsimore Kompetente Digjitale⁴⁶ mund të shërbejë si udhëzues pasi përfshin shtatë elementë kryesorë dhe mjetin SELFIE⁴⁷ me të cilat shkollat mund të zhvillojnë strategjitë e tyre digjitale për të përmirësuar mësimdhënien-të mësuarit dhe sigurinë në internet. Mjeti ofrohet edhe në gjuhën maqedonase.

Mësuesit, si prindër janë të rëndësishëm sepse ata mund të mbikëqyrin aktivitetet në internet të nxënësve/fëmijëve të tyre. Në Vlerësimin Bazë të Studimit të CRPM *“Passage4Prevent: përdorimi i arsimit për të parandaluar radikalizimin e të rinjve onlajn”*, 69.3% e të anketuarve thanë se janë miq me mësuesit e tyre dhe 85.9% janë miq me prindërit e tyre në rrjetet sociale. Pa ndërhyrë në lirinë e mendimit dhe fjalës në angazhimin në internet të

⁴⁵ European Commission. *Digital Competence Framework for Educators*. 2017, në dispozicion në internet: <https://ec.europa.eu/jrc/en/digcompedu>

⁴⁶ <https://ec.europa.eu/jrc/en/digcomporg>

⁴⁷ Shkollat bëhen digjitale https://ec.europa.eu/education/schools-go-digital_mk

nxënësve të tyre, mësuesit mund të luajnë një rol monitorues në fazat e hershme të radikalizimit duke vëzhguar angazhimin në internet të nxënësve të tyre. Përmbajtja e përbashkët dhe diskutimet në internet mund të jenë disa nga treguesit e ndryshimeve radikale ideologjike të nxënësit. Mësuesit gjithashtu mund të krijojnë hapësirë digjitale për të rinjtë, për t'i hequr ato nga hapat e mëtejshëm drejt radikalizimit. Çfarë është më shumë në angazhimin e mediave sociale, mësuesit që janë të motivuar dhe duan të jenë agjentë aktivë të ndryshimit mund të përdorin platformën e tyre për të ndarë përmbajtje alternative/pozitive narrative (fotografi, video dhe blogje) që promovojnë mesazhe kundër radikalizimit.

Drejt një Politike të Sigurisë në internet

Për të krijuar një politikë të sigurisë në internet duhet të zbatohet një qasje gjithëpërfshirëse që konsiston në ndryshime legislative, kërkesa të zhvillimit profesional dhe përgjigje të politikave në nivelin e shkollës. Më poshtë janë rekomandimet që Ministria e Arsimit si organ politikëbërës, Byroja për Zhvillimin e Arsimit si një organ i trajnimit të mësuesve dhe zhvillimit të kurrikulës dhe shkollat si organizata të ofrimit të shërbimeve mund të marrin në periudhën e ardhshme në mënyrë që të ndërtohet qëndrueshmëria ndaj radikalizimit në internet.

Përgjigja legislative

Ligji për Arsimin fillor⁴⁸ dhe Ligjin për Arsimin e mesëm⁴⁹ nuk ka përgatitur ndonjë kërkesë të sigurisë në internet, as privatësi ose mbrojtje të të dhënave personale përveç të dhënave që mblidhen dhe mbahen nga vetë shkollat (e ashtuquajtura statistikë arsimore). Për këtë qëllim, ndryshimet legislative të të dy ligjeve janë të nevojshme për të adresuar sigurinë e nxënësit në internet, kërkesat që çdo shkollë duhet ta plotësojë në mënyrë që të sigurojë një mjedis digjital të sigurt për të mësuarin dhe kompetencat digjitale që stafi mësimdhënës duhet të marrë. Për këtë qëllim, Korniza **DigiComp2.0**, Korniza **DigiEduComp**, duhet të përdoren si harta për reformën. Për më tepër, provimi për Drejtorin e shkollës duhet të rishikohet për të përfshirë në Modul: Teorinë e organizimit ku politika e sigurisë në shkollë në internet do të jetë një nga çështjet e trajtuara sipas Kornizës **DigiCompOrg**.

⁴⁸ <https://mon.gov.mk/download/?f=zakon%20za%20osnovnoto%20obrazovanie%208.10.docx>

⁴⁹ <https://mon.gov.mk/download/?f=Zakon%20za%20srednoto%20obrazovanie%20%2008.10.2020.docx>

Zhvillimi profesional dhe përgjigja e kurrikulës

Analiza e mësipërme tregoi se programit mësimor i mungon përmbytja e rëndësishme e sigurisë në internet. Byroja për Zhvillimin e Arsimit duhet ta zhvillojë atë dhe të përfshihet në kurse të detyrueshme. Çfarë rekomandohet veçanërisht për të shtuar përmbytje në lidhje me sigurinë siç janë mbrojtja e pajisjeve, mbrojtja e të dhënave personale dhe privatësisë, mbrojtja e shëndetit dhe mirëqenies. Përmbytja radikale duhet të përdoret në ushtrime për ndërtimin e aftësive të të menduarit kritik, ndërsa kur mendohet zhvillimi i përmbytjes digjitale duhet të stimulohet krijimi i narrativave alternative pozitive.

Njohuritë digjitale të stafit mësimdhënës duhet të rriten përmes trajnimit por gjithashtu roli aktiv i mësuesve si agjentë të sigurisë në internet duhet të përshkruhet në politikën e shkollës për sigurinë në internet. Kjo do të rrisë pasqyrën për mësuesit dhe roli i tyre do të njihet nga nxënësit, i cili aktualisht siç tregojnë hulumtimet është shumë i ulët. Në këtë proces, zgjedhja e një mësuesi si udhëheqës i sigurisë elektronike do të ndihmonte në zbatimin e politikës në secilën shkollë. Sapo të jenë zhvilluar politikat e e-sigurisë të nivelit shkollor, shkollat duhet të marrin në konsideratë marrjen e pjesës tjetër të stafit duke e shpjeguar rëndësinë e e-sigurisë dhe duke organizuar trajnime rreth përdorimit të tyre të sigurt dhe të përgjegjshëm të përdorimit të internetit dhe politikave të e-sigurisë së shkollës..

Përgjigja e politikës së sigurisë elektronike në nivelin e shkollës

Secila shkollë duhet të zhvillojë politikën e saj të sigurisë elektronike, ose duke përdorur mjetin SELFIE ose duke ndjekur listën e kontrolluar të dhënë në Shtojcën 1 të këtij dokumenti. Politika duhet të përfshijë mësues të caktuar përgjegjës për koordinimin dhe zbatimin e politikës së e-sigurisë. Por meqenëse është një diskutim mbi politikat shkollore rreth parimeve të përgjithshme të e-sigurisë si dhe çfarë hapash duhet të ndërmerren nëse lind një çështje e e-sigurisë mund të përfshihen në takimet e rregullta të stafit mësimor dhe në klasën master së bashku me nxënësit. Pasja e e-sigurisë në agjendën e takimeve të mësuesve dhe prindërve dhe mbledhjeve të këshillit të shkollës do të rrisë dukshmërinë e politikës së sigurisë elektronike në shkollë, si edhe do të kontribuojë në një qëndrueshmëri më

të zgjeruar ndaj radikalizimit në internet. Arsyeja do të ishte të jepeshin shpjegime se pse shkollat janë të interesuara për sigurinë elektronike në shkollë dhe në shtëpitë e nxënësve dhe për të rritur besimin tek mësuesit nga nxënësit.

Shkollat duhet të adresojnë e-sigurinë në një nivel organizativ. Për këtë qëllim, secila shkollë duhet të ketë një mbrojtje ndaj virusit, kriptim të të dhënave personale dhe faqen e internetit të shkollës të siguruar, dhe të mos përfshijë informacione personale për stafin ose nxënësit dhe imazhe të identifikueshme. Pastaj, shkolla duhet të zgjedhë midis mbylljes së përmbajtjes që është e dëmshme ose përdorimit të më pak filtrave për të ndihmuar nxënësit në menaxhimin e rreziqeve në internet se sa t'i shmangë ato në shkollë dhe t'u ekspozohet atyre diku tjetër.

Politika e shkollës duhet të përfshijë përdorimin e mjeteve të tilla si Marrëveshja shtëpi-shkollë, e cila është nënshkruar nga prindi, nxënësi dhe mësuesi (ju lutemi shikoni shembullin në shtojcën 2) dhe marrëveshjen e përdoruesit të stafit që përshkruan se çfarë është e përshtatshme dhe profesionale për stafin në aspektin e sjelljes së tyre në internet.

Së fundmi, shkollat duhet t'i marrin parasysh politikën e pranueshme të përdorimit dhe të marrin në konsideratë meritat që ato azhurnohen çdo vit në mënyrë që çdo shqetësim i ri digjital të mund të integrohet. Politikën e Përdorimit të Pranueshëm zakonisht përfshijnë rregulla dhe këshilla për nxënësit në: fikjen e ekranit dhe informimin e një të rrituri nëse gjen diçka të pakëndshme ose shqetësuese në internet; prekjen e skedarëve që nuk janë të tyre; të qenit i respektueshëm për njerëzit e tjerë në internet; dërgimi i mesazheve abuzive ose të papërshtatshme; dhënia e detajeve personale që mund t'i identifikojnë ato ose vendndodhjen e tyre; vendosja e fotove të tyre në internet; mohimi i hyrjes tek individët e panjohur; bllokimi i komunikimeve të padëshiruara; dhe cilësimet e privatësisë, siguria dhe fjalëkalimet.

Shtojca 1: Lista e Kontrollit për Politikën e Shkollës për Siguri Elektronike

	Definitivisht në vend	Ka nevojë për rishikim dhe vëmendje	Jo në vend
Epërsi dedikuar sigurisë elektronike			
Një politikë e-sigurisë e cila azhurnohet rregullisht			
Politikë e pranueshme e përdorimit për nxënësit			
Një marrëveshje për përdoruesit e kuadrit			
Sistemet e menaxhuara			
Trajnime të rregullta të personelit			
Siguria elektronike si pikë e rendit të ditës në takimet e shkollës			
Trajnim për të gjitha grupet e kuadrit			
Kontrata e marrë në shtëpi			
Siguria elektronike në rendin e ditës në takimet prindër-mësues			
Siguria elektronike në rendin e ditës në mbledhjet e këshillit shkollor			

Shtojca 2: Kontrata e marrë në shtëpi

Kjo marrëveshje rregullon përdorimin e pajisjeve inteligjente, kompjuterëve dhe internetit në familjen e _____ Rregullat e përcaktuara në këtë marrëveshje zbatohen për anëtarët e familjes të shprehur më poshtë: Prindërit _____ dhe _____ fëmijët _____ dhe _____ dhe _____

Rregullat e vendosura në këtë marrëveshje zbatohen gjithashtu për mysafirët në shtëpinë e familjes që përdorin internetin.

Kompjuterët, pajisjet inteligjente dhe interneti do të përdoren për të informuar, mësuar dhe komunikuar me qëllimet më të mira dhe në një mënyrë që nuk do ta dëmtojë askënd.

Kompjuterët, pajisjet inteligjente dhe interneti do të përdoren brenda një kohe të arsyeshme të ditës dhe për kohëzgjatjen e specifikuar nga prindërit.

Nuk lejohen faqet e internetit që kanë përmbajtje të papërshtatshme dhe të dhunshme që mund të shqetësojnë fëmijët. Prindërit duhet të njoftohen kur të gjendet një përmbajtje e tillë.

Përmbajtja e papërshtatshme dhe e dhunshme nuk lejohet të shkarkohet dhe ruhet në një kompjuter ose pajisje të zgjuar. Nëse kjo ndodh, prindërit duhet të njoftohen.

Të gjithë profilet që fëmijët përdorin në rrjetet sociale duhet t'u raportohen prindërve.

Nuk lejohet përdorimi i profileve sekrete dhe false në mediat sociale.

Mos shpërndani informacione dhe të dhëna personale në faqet e dyshimta të internetit ose me të panjohur në mediat sociale.

Shmangni takimet fizike me njerëz në internet që nuk dihen. Nëse ka një propozim për një takim të tillë, prindërit duhet të informohen, dhe nëse është e nevojshme takimi duhet të jetë në prani të një prindi ose të rrituri në një vend publik.

Mos ndani numrat e telefonit me të huajt në internet dhe përgjigjuni telefonatave nga të huajt. Nëse ka një thirrje apo kërkesë të tillë për një telefonatë, njoftoni prindërit.

Komunikimi në internet ose media sociale duhet të jetë i sjellshëm, pa fjalë dhe përmbajtje fyese. Përdorimi i fjalëve dhe përmbajtjeve të tilla duhet t'u raportohet prindërve.

Shkarkimi dhe instalimi i softuerit pa lejen e prindërve, si dhe përmbajtja e paligjshme nga faqet e internetit nuk lejohet.

Pajtueshmëria me këto rregulla zbatohet gjithashtu kur përdorni internet diku tjetër (te një mik, internet kafe, shkolla, hapësira publike, etj.)

Mosrespektimi i këtyre rregullave do të aktivizojë sanksionet më poshtë: ⁵⁰

NËNSHKRIMI I FËMIJËVE:

NËNSHKRIMI I PRINDËRVE:

⁵⁰ Shembujt nga sanksionet përfshijnë: marrjen e kompjuterit ose pajisjes inteligjente për një periudhë të caktuar kohe ose për një kohë të pacaktuar, ndalimin e përdorimit të internetit, kufizimin e kohës së kaluar në internet, etj, në varësi të gravitetit të shkeljes.

Shtojca 3: Marrëveshja e Përdoruesit të Kuadrit ⁵¹

Ju lutemi plotësoni, nënshkruani dhe shënoni datën në këtë Formular të Marrëveshjes së Përdorimit të Kuadrit, i cili konfirmon marrëveshjen tuaj për të ndjekur detyrimet dhe përgjegjësitë e përshkruara në këtë dokument. Detyrimet dhe përgjegjësitë kryesore janë:

- I gjithë përdorimi i ICT duhet të jetë i përshtatshëm për mjedisin shkollor
- Fjalëkalimet do të jenë konfidenciale
- Zbatohen parimet e konfidencialitetit, privatësisë dhe të drejtës së kopjimit.

Nëse keni ndonjë pyetje në lidhje me marrëveshjen, jeni të inkurajuar t'i diskutoni ato me menaxherin e sigurisë në internet ose drejtorin përpara se të nënshkruani. Pasi të nënshkruhet, kjo formë duhet të kthehet në zyrën e shkollës për t'iu kaluar menaxherit të sigurisë në internet për regjistrimin e të dhënave të kuadrit.

Një kopje e formularit të nënshkruar do t'ju dorëzohet.

Ju lutemi shënoni një -

- ☐ Besoj se kam njohuri të mjaftueshme për të mbikëqyrur në mënyrë të sigurt përdorimin e bërë nga nxënësit në kujdesin tim për rrjetin kompjuterik të shkollës, pajisjet e hyrjes në internet, kompjuterët dhe pajisjet/mjetet e tjera të ICT-së shkollore.
- ☐ Unë kërkoj trajnim shtesë/zhvillim profesional në mënyrë që të mbikëqyr në mënyrë të sigurt përdorimin e bërë nga nxënësit në kujdesin tim për rrjetin kompjuterik të shkollës, pajisjet e hyrjes në internet, kompjuterët dhe pajisjet/pajisjet e tjera të ICT-së shkollore.

⁵¹ Ky është një shembull i marrëveshjes për përdorim të kuadrit nga Zelanda e Re, i disponueshëm në internet:

http://www.cybersafety.org.nz/kit/Use%20Agreements/agreements/staff_ua.html

Marrëveshja e përdorimit

Unë kam lexuar dhe jam në dijeni të detyrimeve dhe përgjegjësi të përshkruara në këtë dokument të Marrëveshjes së Përdorimit onlajn të Sigurisë së kuadrit, një kopje e të cilit jam këshilluar ta mbaj për referencë. Këto detyrime dhe përgjegjësi kanë të bëjnë me sigurinë në internet të nxënësve, komunitetit shkollor dhe mjedisit shkollor.

Unë gjithashtu e kuptoj se shkeljet e kësaj Marrëveshjeje të Përdorimit online të Sigurisë së Kuadrit do të hetohen dhe mund të rezultojnë në masa disiplinore, dhe kur kërkohet, referim në zbatimin e ligjit.

Emri:

Detyra në shkollë:

Nënshkrimi:

Data:

Shtojca 4: Politikat e Përdorimit të Pranueshëm⁵²

Qëllimi

Qëllimi i kësaj Politike të Përdorimit të Pranueshëm është të sigurojë që nxënësit të përfitojnë nga mundësitë e të mësuarit të ofruara nga burimet e shkollës në internet në një mënyrë të sigurt dhe efektive. Përdorimi dhe aksesimi i internetit konsiderohet si burim dhe privilegj i shkollës.

Parashikohet që përfaqësuesit e shkollës dhe prindërve të rishikojnë rregullisht AUP-në. Para regjistrimit, AUP duhet të lexohet me kujdes për të siguruar që kushtet e përdorimit janë pranuar dhe kuptuar. Supozohet se prindi i pranon kushtet e AUP-së nëse shkolla nuk është njoftuar posaçërisht.

Qëllimi i kësaj Politike të Përdorimit të Pranueshëm është të sigurojë që nxënësit të përfitojnë nga mundësitë e të mësuarit të ofruara nga burimet e shkollës në internet në një mënyrë të sigurt dhe efektive. Përdorimi dhe aksesimi i internetit konsiderohet si burim dhe privilegj i shkollës.

Parashikohet që përfaqësuesit e shkollës dhe prindërve të rishikojnë rregullisht AUP-në. Para regjistrimit, AUP duhet të lexohet me kujdes për të siguruar që kushtet e përdorimit janë pranuar dhe kuptuar. Supozohet se prindi pranon kushtet e AUP-së nëse shkolla nuk është njoftuar posaçërisht.

Politika e Sigurisë Onlajn në Shkollë

Shkolla përdor një numër mjetesh brenda politikës së saj të sigurisë në internet.

⁵² Ky është një shembull i Politikës së përdorimit të pranueshëm të shkollës kombëtare Powerstown edukojmë së bashku, nga Irlanda

Përgjithësisht

- Sesionet në internet do të mbikëqyren gjithmonë nga një mësues.
- Shkolla do të monitorojë rregullisht përdorimin e internetit të nxënësve.
- Nxënësve dhe mësuesve do t'u ofrohet trajnim në fushën e sigurisë në Internet.
- Ngarkimi dhe shkarkimi i softuerit të pa aprovuar nuk do të lejohet.
- Softueri për mbrojtjen e viruseve do të përdoret dhe azhurnohet rregullisht.
- Përdorimi i USB-ve personale, CD-ROM, ose mediave të tjera të ruajtjes digjitale në shkollë kërkon lejen e një mësuesi.
- Nxënësit do të trajtojnë të tjerët me respekt në çdo kohë dhe nuk do të ndërmarrin asnjë veprim që mund ta sjellë shkollën në mosrespekt.
- Është e rëndësishme që prindërit/kujdestarët dhe nxënësit të jenë të vetëdijshëm për Politikën tonë të Anti-Bullizmit në lidhje me mediat sociale;

Incidente të izoluara ose të njehershme të sjelljes negative të qëllimshme, duke përfshirë një mesazh me shkrim ofendues ose lëndues ose mesazhe të tjera private, nuk bien brenda përkufizimit të ngacmimit dhe duhet të trajtohen, sipas rastit, në përputhje me kodin shkollor të sjelljes.

Sidoqoftë, në kontekstin e kësaj politike, vendosja e një mesazhi, imazhi ose deklaratë publike një herë ofenduese ose lënduese në një faqe të rrjetit social ose në një forum tjetër publik ku ai mesazh, imazh ose deklaratë mund të shihet dhe/ose përsëritet nga njerëz të tjerë do të konsiderohet si sjellje ngacmimi

World Wide Web

- Nxënësit nuk do të vizitojnë me qëllim faqet e Internetit që përmbajnë materiale të pahijshme, të paligjshme, urrejtëse ose përndryshe të kundërshtueshme.
- Nxënësit do të raportojnë aksesin e rastësishëm të materialeve të papërshtatshme në përputhje me procedurat e shkollës.
- Nxënësit do të përdorin internetin për qëllime arsimore vetëm gjatë orës së mësimi. Të gjitha faqet e internetit do të verifikohen nga mësuesi i klasës.

- Nxënësit nuk do të kopjojnë informacionin në detyra dhe nuk do të pranojnë burimin (plagjiaturë dhe shkelje e të drejtës së autorit).
- Nxënësit kurrë nuk do të zbulojnë ose publikojnë informacione personale.
- Shkarkimi i materialeve ose imazheve që nuk janë të rëndësishme për studimet e tyre, është në kundërshtim të drejtpërdrejtë me politikën e pranueshme të shkollës.
- Nxënësit do të jenë të vetëdijshëm se çdo përdorim, përfshirë shpërndarjen ose marrjen e informacionit, lidhur me shkollën ose personale, mund të monitorohet për veprimtari të pazakontë, siguri dhe/ose arsye të menaxhimit të rrjetit.

Email / Google Drive / Internet Chat

- Nxënësit duhet të nënshkruajnë një marrëveshje me shkrim për shtëpinë çdo vit, me prindërit dhe mësuesin e klasës, përpara se të hyjnë në llogaritë e shkollës.
- Nëse një nxënës merr ndonjë email të papërshtatshëm, ai/ajo duhet të informojë mësuesin e klasës dhe një prind/kujdestar.
- Nxënësit nuk do të dërgojnë ose marrin asnjë material që është i paligjshëm, i turpshëm, shpifës ose që ka për qëllim të fyejë ose frikësojë një person tjetër.
- Nxënësit nuk do të zbulojnë detajet personale të tyre ose të personave të tjerë, të tilla si adresat ose numrat e telefonit, fotografitë ose fjalëkalimet.
- Nxënësit nuk do të organizojnë kurrë një takim ballë për ballë me dikë që e njohin vetëm përmes postës elektronike ose internetit.
- Nxënësit nuk do të kenë qasje në dhomat e bisedave, forume diskutimi, mesazhe ose forume të tjera të komunikimit elektronik.

Web 2.0

Me ardhjen e Web 2.0, Interneti është bërë një sistem komunikimi dy drejtimësh për shkollën dhe komunitetin e gjerë. Shërbime të tilla si Scribd, Class Dojo, Facebook, Wordpress, Twitter dhe media të tjera sociale po përdoren nga shkolla për të komunikuar me prindërit dhe gjithashtu që prindërit të komunikojnë me shkollën. Këto shërbime, janë pjesë e shërbimeve tona në internet dhe e gjithë përmbajtja që vendoset në këto shërbime bie nën këtë politikë. Për shembull, çdo përmbajtje në llogarinë e

shkollës Scribd ndjek të njëjtat rregulla sigurie, p.sh. shfaqja e fotografive, videove, etj.

- Shumë faqe të mediave sociale kanë kërkesa minimale për moshën. Ndërsa shkolla nuk do ta monitorojë këtë, ne do të këshillojmë prindërit të mos lejojnë që fëmijët e tyre të kenë llogari personale në Facebook, Twitter, etj. Derisa të jenë në moshën e duhur. Shumë faqe të mediave sociale do të përdoren nga mësuesit në klasë, për shembull, Twitter. Sidoqoftë, të gjitha ndërveprimet do të jenë nën mbikëqyrjen e mësuesit.
- Prindërit dhe kujdestarët inkurajohen të kontrollojnë rregullisht aktivitetin/gjurmën digjitale të fëmijës së tyre në internet. Prindërit inkurajohen të kontrollojnë aplikacionet e mediave sociale (p.sh. Facebook, Snapchat, Viber, Whatsapp, Instagram etj) në telefona celularë dhe pajisje elektronike për të siguruar që ata janë të vetëdijshëm për ndërveprimin në internet të fëmijës së tyre dhe të miratojnë të njëjtën gjë.
- Ju lutemi mos “etiketoni” fotografi ose ndonjë përmbajtje tjetër që identifikon ndonjë fëmijë ose personel në shkollë.
- Nëse jeni duke ngarkuar një fotografi, sigurohuni që ajo të mos identifikojë fëmijën në asnjë mënyrë. Ju lutemi sigurohuni që madhësia e fotografisë të mbahet sa më e vogël (jo më e madhe se 800x600 piksel).
- Ju lutemi sigurohuni që mesazhet dhe komentet në internet për shkollën të jenë të respektueshme. Çdo mesazh i shkruar në mediat sociale trajtohet në të njëjtën mënyrë si mesazhi i shkruar për shkollën.
- Shmangni çdo bisedë negative në lidhje me fëmijët, stafin ose prindërit në llogaritë e mediave sociale.
- Ju lutemi mos shtoni reklama në murin tonë pa lejen paraprake të porositësit.
- Mosrespektimi i rregullave të mësipërme do të rezultojë në një ndalim të përhershëm të llogarive tona të mediave sociale.

Uebfaqja e shkollës

- Ju lutemi vini re se pikat e mëposhtme vlejnë për faqen e shkollës dhe profilet e mediave sociale, duke përfshirë por pa u kufizuar në Facebook, Twitter, YouTube, Scribd dhe Google+
- Nxënësve do t'u jepet mundësia të botojnë projekte, vepra arti ose punë shkollë në World ide Web në përputhje me politikat e qarta dhe proceset e miratimit në lidhje me përmbajtjen që mund të ngarkohet në faqen e shkollës
- Uebfaqja do të kontrollohet rregullisht për të siguruar që nuk ka përmbajtje që cenon sigurinë e nxënësve ose të personelit.
- Uebfaqe duke përdorur pajisje të tilla si libra për vizitorë, tabela njoftimesh ose uebblogje do të kontrollohen shpesh për të siguruar që ato nuk përmbajnë të dhëna personale
- Publikimi i punës së nxënësit do të koordinohet nga një mësues.
- Puna e nxënësve do të shfaqet në një kontekst arsimor në faqet e internetit
- Shkolla do të përpiqet të përdorë fotografi digjitale, audio ose video klipe të përqendrimit në aktivitete në grup. Do të përdoren edhe fotografi, klipet audio dhe video. Videoklipet nuk do të mbrohen me fjalëkalim.
- Informacioni personal i nxënësit, përfshirë adresën e shtëpisë dhe detajet e kontaktit do të hiqen nga uebfaqet e shkollës.
- Uebfaqja e shkollës do të shmangë botimin e mbiemrit të individëve në një fotografi.

Telefonat celularë/pajisjet elektronike

- Përdorimi i telefonave celularë/pajisjeve elektronike duhet të respektojë politikën e telefonisë mobile/pajisjeve elektronike.
- Shkolla pranon dobinë dhe praktikën e telefonave celularë/pajisjeve elektronike dhe njeh potencialin e tyre si një burim arsimor.
- Shumë karakteristika në celularët/pajisjet elektronike si Organizuesi (kalendari, kalkulatori, konvertuesi etj.) Aplikacionet (regjistruar zëri, kronometër, redaktues imazhesh, video regjistruar) apo edhe Alarme janë shumë të dobishme dhe mund të përdoren nën drejtimin e mësuesit të klasës. Nëse dhe kur ndodhë ndonjë aktivitet i tillë prindërit do të njoftohen paraprakisht.

- Nxënësit që përdorin teknologjinë e tyre në shkollë, të tilla si lënia e një telefoni celular të ndezur ose përdorimi i tij në klasë është në kundërshtim të drejtpërdrejtë me politikën e pranueshme të shkollës.
- Nxënësit që dërgojnë mesazhe me tekst shqetësues, është një shkelje e drejtpërdrejtë e përdorimit bazuar në politikën e pranueshme të shkollës.
- Marrja e paautorizuar e imazheve me një aparat fotografik të telefonit celular ose pajisje elektronike, në qetësi apo lëvizje është në kundërshtim të drejtpërdrejtë me politikën e pranueshme të shkollës.