

PROBLEMATIKA SPLETNE VARNOSTI V ŠOLAH

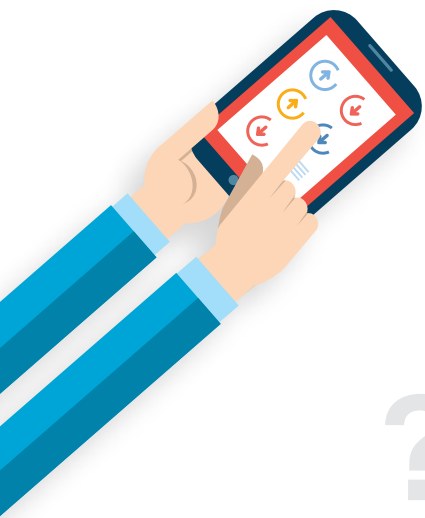
SMERNICE ZA VODSTVA ŠOL





PROBLEMATIKA SPLETNE VARNOSTI V ŠOLAH

SMERNICE ZA VODSTVA ŠOL



?

?

!

?

?

?

!

?

KAZALO

Pojav informacijske tehnologije na šolah	7
Vloga šole pri uvajanju informacijske tehnologije	7
Varna in odgovorna raba interneta ter povezane aktivnosti	9
Oblike zlorab na internetu	11
Odgovornost za nedopustno ravnanje	12
Ukrepanje ob incidentu	14
Ravnatelj	15
Učitelj	18
Starši	19
Učenec	19
Kazniva dejanja na internetu	21
Primeri zlorab in rešitev	22

UVOD

Gotovo ste že slišali zgodbo o osnovnošolki Ani, ki je na omrežju zasledila svoje fotografije, ali o Mateju, ki so ga sošolci pretepli zaradi razširjanja laži na lažnih profilih, ali zgodbo o dijakinji Maji, ki se je z družino preselila v nov kraj, ker so novi sošolci ponovno izbrskali njeno staro fotografijo zgoraj brez, ali zgodbo o Luki, ki je končal s šolanjem zaradi zasvojenosti z igranjem iger, ali zgodbo o učitelju Janezu, ki je izgubil službo zaradi objav na družabnem omrežju, ali o učiteljici Veroniki, ki je končala z delom na šoli, ker ni prenesla osebnih pritiskov zaradi objav posnetkov na Youtubu, ali zgodbe o ...

Vsaka šola ima svoje zgodbe o Ani, Mateju, Luki ali učiteljici Veroniki in ta priročnik je namenjen ravno vodstvom šol oziroma ravnateljem, v določeni meri pa tudi staršem učencev in dijakov. A ne za to, da teh zgodb ne bi bilo več, saj je to nemogoče, ampak da boste v vodstvih šol pripravljeni, preden se bo neljubi dogodek začel odvijati, da bo takih pripetljajev čim manj, da boste nanje pripravili tudi starše in da boste znali trezno ravnati ob podobnih situacijah ter navsezadnje, da boste poskušali ustvarjati šolo z učenci in učitelji, ki se bodo zavedali varne in odgovorne rabe interneta.



POJAV INFORMACIJSKE TEHNOLOGIJE NA ŠOLAH

Dejstvo je, da si šole brez prisotnosti informacijske tehnologije ne moremo več predstavljati. V to dejstvo nas tiščita stalna hitrost razvoja družbe in tehnološka obarvanost vseh komponent razvoja.¹ Učenci, ki se danes šolajo v osnovni šoli, bodo po zaključenem podiplomskem študiju začeli z delom okoli leta 2030 in bodo poklic opravljali do okoli leta 2080. Ali si znamo predstavljati, kakšne kompetence jim mora šola dati, da bodo zanimivi na trgu dela? Digitalna pismenost je gotovo ena izmed pomembnih kompetenc, ki jo spodbuja tudi EU v svojih usmeritvah. Osvajanje digitalne kompetence pa brez informacijske tehnologije ni možno.

Vloga šole pri uvajanju informacijske tehnologije

Informacijska tehnologija se na šolah pojavlja v najrazličnejših oblikah. Bodisi kot izključno tehnologija v obliki namiznih in prenosnih računalnikov, tablic, mobilnih telefonov, digitalnih tabel, fotoaparatom, kamer in ostalih digitalnih učnih pripomočkov bodisi kot digitalna vsebina v obliki elektronskih učbenikov in delovnih zvezkov, drugih gradiv, učnih portalov, aplikacij, igrice, videoposnetkov, MOOC-ov², učnih družabnih omrežij in drugih storitev, ki jih omogoča internet.

Iz statistik lahko razberemo, da je računalniška opremljenost slovenskih šol

¹ Vir: Aberšek, Flogie, Šverc, 2015. Sodobno kognitivno izobraževanje in transdisciplinarni modeli učenja: pedagoška strategija.

² MOOC je kratica za Massive Open Online Course, kar pomeni množični spletni tečaj, ki poteka odprto na internetu za različne udeležence (tudi več tisoč).

v letu 2015 okoli povprečja EU ter da ima večina od 24.000 učiteljev ustrezne kompetence za uporabo informacijske tehnologije pri poučevanju, čeprav jo pri delu z učenci redno uporablja samo okoli 30 odstotkov; na drugi strani pa pri pripravi na pouk in druge dejavnosti informacijsko tehnologijo uporablja več kot 80 odstotkov učiteljev.³

Večina informacijske tehnologije vstopa v šolo načrtno, to je z nabavo in namestitvijo same tehnologije ali s pripravo in ponujanjem elektronskih vsebin, s pomočjo katerih poteka izobraževalni proces.

Ko šola lastno informacijsko tehnologijo, npr. računalnik ali tudi aplikacijo za izvajanje izobraževalnega procesa, poveže z internetom, omogoči dostop do vseh vsebin interneta, to je do vseh zelenih spletnih strani in storitev, kakor tudi do vseh neželenih in neprimernih ali celo prepovedanih vsebin. Ali lahko šola na lastnih računalnikih onemogoči prikazovanje neželenih vsebin? Odgovor je pritrdilen, saj obstajajo različne tehnične nastavitve, ki uporabnikom v omrežju šole dovoljujejo dostop le do izključno zelenih vsebin oziroma se uporabnikom prepove dostop na posamezne spletne strani.⁴ Šola se mora zavedati, da tehnike omejevanja niso 100 % učinkovite, saj so možni različni obvodi omejitev, omejitve pa običajno še spodbudijo učence, da poskušajo kršiti pravila.

Informacijska tehnologija vstopa na šolo tudi nenadzorovano. V mislih imamo predvsem mobilno tehnologijo, kot so telefoni in tablice, ki jih s seboj v šolo prinesejo učenci. Nad vsebinami in storitvami, ki se prikazujejo na teh napravah, šola skorajda nima možnosti tehničnega omejevanja ali nadzora, razen v primeru, ko so te naprave priključene na šolsko brezžično omrežje. A kot je znano, imajo mobilne naprave zelo pogosto lasten dostop do interneta preko t. i. podatkovnega paketa pri operaterju mobilne telefonije, ki omogoča tako rekoč neomejen internetni dostop.

V primeru, ko šola nima nadzora nad tehnologijo in vsebinami oziroma storitvami, lahko pride do nepredvidljivih posledic, saj npr. tak sodoben telefon omogoča popoln dostop do interneta, nudi možnost visokokakovostnega snemanja fotografij in videoposnetkov, s široko paleto aplikacij in skoraj neomejeno možnostjo povezljivosti med uporabniki pa je z njim mogoče narediti mnogo dobrega in tudi slabega.

Z uvajanjem in uporabo informacijske tehnologije se na šoli zagotovo izboljšujejo metode poučevanja in učenja ter poskuša okrepiti učno okolje tako za učitelje kot za učence. Pri tem pa moramo upoštevati, da zmogljiva in prefinjena informacijska tehnologija v vseh možnih oblikah vključno z rabo interneta sproža vrsto pravnih, etičnih, tehničnih in organizacijskih vprašanj. Tako se odpira široko polje potreb po formalnem urejanju uporabe informacijske

³ Vir: STA <https://www.sta.si/2174243/racunalniska-opremljenost-slovenskih-sol-na-ravni-eu> (13. 9. 2015).

⁴ Npr. šola omeji dostop do nekaterih družabnih omrežij tako, da ustvari omejitve na omrežnih stikalih oziroma na računalnike namesti posebno programsko opremo, ki to omogoča.

tehnologije na šoli kot tudi po uvajanju neformalnih vzvodov in vzorcev primerne vedenja. Neformalno in tisto, kar sprejmejo učenci za svoja pravila ali svoj način vedenja, presega formalno ureditev in ravno to omogoča normalno sobivanje udeleženi v izobraževalnem procesu šole, sobivanje med vodstvom šole, učitelji, učenci in njihovimi starši.

Varna in odgovorna raba interneta ter povezane aktivnosti

Ko govorimo o varni rabi interneta, jo povezujemo s spletno varnostjo, ki je pogosto napačno razumljena in je zato z nekaj primeri lažje opredeliti, kaj to ni. Spletna varnost predvsem ne pomeni blokiranja spletnih strani, prekomernega nadzorovanja prometa na internetu, striktnega omejevanja uporabe interneta in kriminalizacije družabnih omrežij (kot so npr. Facebook, Instagram, Twitter).

Več o družabnih omrežjih in njihovem delovanju preberite na spletni strani Safe.si:
<http://www.safe.si/podrocja/druzabna-omrežja>.

Šole se pogosto zatečejo v hitre tehnične rešitve in uporabo prej omenjenih načinov omejevanja interneta, da bi ohranile svoje učence in šolo varne. Ne zavedajo pa se, da obstajajo na internetu številne rešitve in navodila, kako obiti še tako zapletene tehnične ovire, ki učencem nato brez ovir omogočijo dostop do vsebin in storitev, ki si jih na šoli ne želijo. Ugotovimo lahko, da tehnično omejevanje običajno ne prinese zelenih rezultatov in ima pogosto nasproten učinek.

Upoštevati moramo, da je spletna varnost predvsem znanje. Star kitajski pregovor pravi: »Daj človeku ribo in si ga nahranil za en dan. Nauči človeka loviti in si ga nahranil za življenje.« Podobno je naravnana tudi spletna varnost, pri kateri blokiranje in omejevanje spletnih vsebin nimata dolgoročnega učinka na učence, temveč delujeta z danes na jutri. Upoštevati moramo tudi, da se tehnologija hitro spreminja. Veliko bolje se obnese izobraževanje, kako naj se učenci varno in odgovorno vedejo na spletu, kar jim bo omogočalo urjenje in pridobivanje veščin o varni in odgovorni rabi interneta, ki jih bodo obdržali celotno življenje.

Upoštevati moramo, da je internet eno izmed najboljših orodij in izjemen pripomoček v izobraževalnem procesu. Učenci se zavedajo količine informacij ter možnih storitev, zato dobesedno srkajo vsebine in izrabljajo možnosti

različnih storitev, ki jih nudi internet. Obenem pa internet predstavlja veliko grožnjo, ko se učenci nepripravljeni in neizobraženi podajo v raziskovanje njegovih vsebin ter storitev, še posebej, če se ne zavedajo posledic lastnih dejanj (npr. kakšne nepopravljive posledice lahko prinese objava grozilnega sporočila ali objava gole fotografije) in če niso izobraženi, kako ravnati v težavnih situacijah (npr. kako naj se učenec odzove, ko se njegova sporna vsebina znajde na internetu, kako naj se odzove na povabilo na srečanje s prijateljem, ki ga pozna le z družabnega omrežja).

Na tem mestu imajo šole pomembno vlogo, saj otroci preživijo tretjino dneva v šoli. Zavedamo pa se, da imajo šole predpisan program izobraževanja, ki se ga morajo držati. Zato se jim pri Safe.si poskušamo čim bolj približati in jim pomagati z delavnicami o različnih temah varne rabe interneta in mobilnih telefonov, ki so sestavljene iz teoretičnega dela, kjer se učence prek predavanja, pogovora in izmenjave izkušenj ter predvajanja videogradiv seznanjajo z osnovnimi koncepti, pravili ter nasveti varne in odgovorne rabe interneta, zadnji del delavnic pa je namenjen praktičnemu delu z različnimi zanimivimi interaktivnimi aktivnostmi.

Priporočeno je, da šola v aktivnosti varne rabe interneta vključi tudi starše, saj ti predstavljajo najbolj pomemben del otrokove vzgoje in edino z njihovim sodelovanjem bo šola uspela doseči uspehe tudi pri učencih. Za starše imamo pri Safe.si pripravljena predavanja s strokovnjaki in praktiki s področja varnosti na internetu z naslovom Internet – ulica v otroški sobi, v okviru katerega predstavimo nekaj tipičnih tveganj, s katerimi se otroci redno srečujejo pri uporabi interneta, oblike vedenja na spletu, ko otroci pogosto ne razumejo povezave med dejanji, ki jih naredijo, in posledicami, ki jih bodo za ta dejanja nosili tudi v »fizičnem« svetlu, in predstavimo nekaj nasvetov, kako se obvarovati pred tveganji in kakšne vzgojne ukrepe uporabiti v povezavi z otrokovo uporabo sodobnih tehnologij.

Safe.si od leta 2005 deluje kot nacionalna točka osveščanja otrok in najstnikov o varni rabi interneta in mobilnih naprav. Naše aktivnosti so namenjene štirim ciljnim skupinam: otrokom, mladostnikom, staršem in strokovnim delavcem (učiteljem, socialnim, mladinskim delavcem ...). Poslanstvo kampanje osveščanja je informiranje mladih uporabnikov interneta ter mobilnih naprav, kako se lahko zaščitijo pred tveganji ter varno in odgovorno uporabljajo splet in druge nove tehnologije.

Oblike zlorab na internetu

Zlorabe na internetu imajo številne oblike, kakor tudi imena, ki so običajno neznana in tuja, zato predstavljamo nekatere najbolj pogoste oblike zlorab. Te zlorabe potekajo s pomočjo katerekoli informacijske tehnologije (računalnikov, mobilnih telefonov, tablic, igralnih konzol), kot tudi preko različnih spletnih strani, družabnih omrežij, iger ali aplikacij na mobilnih napravah.

Spletno nadlegovanje (Cyberbullying) je splošen izraz za izvajanje različnih oblik spletnega nasilja in ustrahovanja, pod katerega lahko strnemo različne oblike, ki jih opisujemo tudi v nadaljevanju.

Sexting označuje pošiljanje golih fotografij prek sporočil ali aplikacij na telefonu. Početje je značilno predvsem za najstnike, ki se fotografirajo goli ali napol goli, nato pa si fotografije najpogosteje s pomočjo mobilnega telefona izmenjujejo z vrstniki.

Spletno zalezovanje (Cyberstalking, stokanje oz. stalking) je zalezovanje oziroma nadlegovanje preko vseh možnih družbenih omrežij, iger, aplikacij in drugih kanalov.

Navezovanje stikov (Grooming) z otroki prek spleta z namenom spolne zlorabe je oblika zlorabe, s pomočjo katere se odrasli pretvarjajo, da so vrstniki svojih žrtev, da bi vzpostavili zaupanje pri mladoletni osebi. Na spletu začnejo pogovor s svojo potencialno žrtvijo in tako poskušajo izvedeti njen naslov, interese, hobije in izkušnje v spolnosti. Z različnimi triki poskušajo otroke zapeljati v pogovore o spolnosti in nazadnje v srečanje v živo.

Objavljanje posnetkov nasilja (Happy slapping) obsega nasilno vedenje do žrtve – npr. klofute (angl. slap) –, kar lahko preraste v grobo fizično nasilje – pretepanje –, ki ga opazovalci posnamejo s telefonom, posnetek pa žrtvi v posmeh objavijo na spletnih straneh, namenjenih izmenjavi multimedijskih vsebin (npr. na Youtube).

Trolanje pomeni objavljanje žaljivih, sovražnih, hujskaških sporočil v spletnih skupnostih, katerih namen je spodbuditi čustvene reakcije udeležencev ali drugače motiti normalno diskusijo o določeni temi oziroma vzbuditi pozornost.

Več izrazov in njihov pomen poiščite na spletni strani [Safe.si](http://www.safe.si) pod nasveti za vsako področje: <http://www.safe.si/nasveti> oziroma pod slovarjem pojmov: <http://www.safe.si/slovar-pojmov>.



ODGOVORNOST ZA NEDOPUSTNO RAVNANJE

Nedopustna ali protipravna dejanja, ki jih povzroči učenec, se najpogosteje imenujejo incident, ki se lahko zgodi na šoli oziroma v prostem času in ga kot takega šole običajno tudi obravnavajo. Zato bomo tudi v nadaljevanju uporabljali ta izraz, ki je sicer v Slovarju slovenskega knjižnega jezika opredeljen kot: »nepričakovan, neprijeten dogodek, ki prekine normalen potek kakega dejanja, dela« oziroma kot: »prepir, spor«, nadalje pa tudi kot »prekoračenje dovoljenega v ravnanju ali vedenju, izgred«.

V primeru incidentov se pogosto išče odgovornost za tako dejanje oziroma ravnanje. A ker je učenec lahko mladoleten in zaradi tega, ker je pod skrbstvom šole, je treba to odgovornost pregledati zelo natančno. Incident, ki se zgodi na šoli, se pravno lahko obravnava glede na starost učenca, ki je incident povzročil, na pravno področje (kazensko ali civilno področje) in glede na vključenost drugih oseb (starši ali zakoniti zastopniki, skrbnik, šola, ustanova).

Kazensko in prekrškovno pravo

Po kazenskem in prekrškovnem pravu mladoletni učenec, ki še ni dopolnil 14 let, ne more biti storilec kaznivega dejanja ali prekrška in v takem primeru kazensko ne odgovarja za storjeno protipravno dejanje. Tudi policija ne bo ukrepala, niti ne bo naredila zapisnika, ampak bo postopek zaključila z ugotovitvijo, da je domnevni storilec mlajši od 14 let.

Po dopolnjenem 14. letu pa je učenec kazensko odgovoren, torej je storilec kaznivega dejanja, sam kazenski oziroma prekrškovni postopek zoper mladoletnika pa je nekoliko drugačen, predvsem pa je v postopek vključen center za socialno delo. Kazenska zakonodaja takega storilca obravnava kot

mlajšega (14 in 15 let) oziroma starejšega mladoletnika (16 in 17 let).

Po dopolnjenem 18. letu postane učenec polnoleten in ga kazenska zakonodaja obravnava kot mlajšega polnoletnika, pri katerem je možna nekoliko milejša obravnava glede sankcij. Pomembno pa je poudariti, da starši za dejanja otroka kazensko ne odgovarjajo v nobenem primeru.

Civilno pravo

V civilnem pravu se presoja morebitna odškodninska odgovornost, pri kateri se presojuje naslednje štiri predpostavke, ki morajo biti, da je ugotovljena odškodninska odgovornost, vse izpolnjene:

- ali je bilo ravnanje nedopustno (npr. protipravno ravnanje ali opustitev ravnanja);
- ali je nastala škoda (npr. povzročitev telesnih ali duševnih bolečin ali strahu drugemu – nepremoženjska škoda oziroma premoženjska škoda);
- ali obstaja vzročna zveza med nedopustnim ravnanjem in nastankom škode (npr. objava fotografije, razkritje podatkov, kraja identitete, nasilje) in
- ali je podana odgovornost obravnavane osebe (subjektivna oziroma objektivna odgovornost).

Pri presojanju odgovornosti učenec, ki je mlajši od 7 let, ni civilno odgovoren za povzročeno škodo, ravno tako ni civilno odgovoren za povzročeno škodo mladoletnik, star med 7 in 14 let, razen če je sposoben razumevanja svojih dejanj.

Mladoletnik, ki je star 14 let in več, pa je popolnoma odgovoren glede na splošna pravila o odgovornosti za povzročeno škodo. Torej odgovarja za svoja dejanja sam.

Starši kot zakoniti zastopniki mladoletnega učenca so civilno odgovorni za škodo, ki jo povzroči njihov otrok, razen če je bil otrok zaupan drugemu, ki zanj odgovarja (npr. skrbnik, šola ali druga ustanova). Do 7. leta starši odgovarjajo objektivno, od 7. do 14. leta pa krivdno solidarno z otrokom.

Torej za škodo, ki jo povzroči mladoletnik od 7. do 18. leta,⁵ odgovarjajo starši, razen če dokažejo, da za nastalo škodo niso krivi. To morajo dokazati starši. Krivda se presoja glede na to, kako so otroka vzgajali, torej glede na njihovo prizadevanje in ne glede na rezultat (ne glede na to, kakšen je otrok dejansko).

Ko je mladoletni učenec pod nadzorstvom skrbnika, šole ali druge ustanove in v tem času stori neko nedopustno ali protipravno ravnanje – incident –, takrat civilno odgovarjajo skrbnik, šola oziroma ustanova, razen če dokažejo,

⁵ Otrok do polnoletnosti še nima lastnih sredstev. Z dopolnjenimi 15 leti pa postane poslovno omejeno sposobna oseba in npr. lahko sklene delovno razmerje ter razpolaga s svojim osebnim dohodkom.

da so opravili nadzorstvo z dolžno skrbnostjo ali da bi škoda nastala tudi pri skrbnem nadzorstvu. V kolikor odgovarja tudi mladoletnik, je odgovornost solidarna. Omenjena nadzorstvena dolžnost se kaže predvsem pri fizičnem nadzoru otrok npr. med poukom, odmori, na letovanjih ipd.

Če nadzorstvo nad mladoletnim učencem ni dolžnost staršev, temveč koga drugega, ima oškodovanec vseeno pravico zahtevati odškodnino od staršev, če je škoda nastala zaradi slabe vzgoje mladoletnika, slabih zgledov ali grdih navad, ki so mu jih dali starši, ali če se tudi sicer škoda lahko pripiše njihovi krivdi.

Ukrepanje ob incidentu

Šola je dolžna nadzorovati učence in izvajati t. i. nadzorstveno dolžnost, ki se razteza na čas, ko učenci prestopijo šolski prag, pa vse do njihovega odhoda domov.⁶ Omenjeno nadzorstveno dolžnost zaposleni v šoli izvajajo med poukom, v odmorih, med izleti ali drugimi dejavnostmi šole izven šole, a v času, ko so učenci zaupani šoli. Sicer se nadzorstvena dolžnost šole v sodni praksi preverja za vsak primer posebej. Do sedaj pa še ni znano, na kakšen način mora šola izvajati nadzorstveno pravico na področju nadzora učenca pri uporabi informacijske tehnologije in interneta.

Šola mora imeti izdelan sistem ukrepov za izvajanje dolžnega nadzorstva v internih aktih in te ukrepe mora tudi izvajati. Med take ukrepe na področju informacijske tehnologije sodita npr. ureditev uporabe mobilnih naprav in zaveza šole izvajanju ukrepov za varno in odgovorno rabo interneta.

Aktivnosti, ki jih učenci izvajajo na internetu z uporabo računalnika ali mobilnih naprav, šola ne more nadzirati neposredno, četudi se zgodijo v času, ko mora šola izvajati nadzorstveno dolžnost. Vodstvo šole mora predvsem vzpostaviti takšne pogoje, da bodo njeni zaposleni lahko izvajali nadzorstveno dolžnost, oziroma mora šola imeti sprejete vzgojni red in pravila šolskega reda oziroma šolska pravila, kjer bodo opredeljeni pričakovano in prepovedano vedenje oziroma ravnanja in ukrepi ter morebitne sankcije ob kršitvah.

Tveganja za povzročitev incidenta s strani učencev z uporabo mobilne naprave so toliko višja, saj je incident, četudi se zgodi v času pouka, lahko popolnoma skrit nadzornemu učitelju. Nasprotno pa je ob očitnem npr. slikovnem snemanju učenca učitelj dolžan ukrepati, saj učenec med poukom ne sme uporabljati telefona. Slednje mora šola v svojih aktih ustrezno prepovedati in predvideti postopek za izročitev sporne naprave. Šola tudi ne more prevzeti odgovornosti za ravnanja učencev, ki se zgodijo na internetu, če jih ne opazi, še manj pa šola ne more prevzeti odgovornosti za ravnanja, ki se zgodijo izven časa nadzorstvene dolžnosti, to je izven pouka, četudi jih počnejo njeni učenci.

⁶ Kot je to opredeljeno v sodbi vrhovnega sodišča (VSL I Cp 4505/2008).

Na kratko smo opisali zgolj nekaj okoliščin, v katerih lahko pride do incidenta ob uporabi informacijske tehnologije, dejanskih primerov pa je izjemno veliko. Zato smo zbrali različne ukrepe in priporočila glede na aktivnosti pred, med in po incidentu, ki se zgodi s pomočjo ali preko informacijske tehnologije na internetu (npr. spletno nasilje, neupravičena objava slikovnega materiala, izsiljevanje ...). Te ukrepe smo razporedili na vloge, ki jih imajo pri incidentu ravnatelj, učitelj, starš in sam učenec s poudarkom na aktivnostih za vodstva šol. Vse omenjene stranke morajo skrbno presoditi intenzivnost protipravnosti oziroma škodljivosti incidenta in v primeru najhujših oblik kršitev brez odlašanja obvestiti in v razreševanje vključiti policijo (113).

Ravnatelj

PRED INCIDENTOM:

Ravnatelj je dolžan zagotoviti ustrezno ureditev in organizacijo dela ter pogojev dela na šoli. Temeljni dokumenti, v katerih šola opredeli možnosti razreševanja incidentov, so vzgojni načrt in pravila šolskega reda oziroma pravilnik o šolskem redu v srednji šoli in šolska pravila, ki jih običajno sprejme svet šole na predlog ravnatelja. Predlagamo, da se v teh splošnih internih aktih šole zapišeta jasna usmeritev šole k nenasilju (tudi) na internetu ter usmeritev k varni in odgovorni rabi interneta, računalnikov in mobilnih naprav. Obenem se mora jasno predvideti ukrepe ob nespoštovanju pravil (npr. protokol izročitve mobilne oziroma druge sporne naprave, ravnanje ob zaznavi nasilja, možnost zadržanja učenca na šoli do prihoda staršev). Obenem se v internih aktih predvidijo tudi proaktivni ukrepi za zmanjšanje tveganj, kot so sodelovanje, dodatno izobraževanje, pozitivna mediacija ipd.

Kot vzgojni moment predlagamo, da ravnatelji pred sprejetjem pravil za širše soglasje k pravilom prosijo tudi učence, ki npr. na razrednih urah obravnavajo predlagana pravila ali celo pripravijo svojo različico pravil in ukrepov ob nespoštovanju.

Vsa sprejeta pravila in interni dokumenti šole naj bodo javno objavljeni in dostopni. Ravno tako sta nujna redno obnavljanje in prenavljanje pravil.

V vsakokratnem letnem delovnem načrtu lahko ravnatelj ustrezno predvidi izobraževanje učencev in učiteljev ter staršev v zvezi z varno in odgovorno rabo interneta v obliki delavnic in predavanj.

Več informacij o delavnicah za učence in predavanjih za starše poiščite na <http://www.safe.si/aktivnosti/izobrazevanja-o-varni-rabi-interneta>.

Šola naj izrazi jasno pripravljenost, da bo pomagala razreševati probleme tudi pri tistih incidentih, ki se zgodijo izven pouka in zanje neposredno ni odgovorna, ampak se zaveda, da so v incident vpleteni njeni učenci, ki so »njeni« 24 ur dnevno in ne samo v času, ko prestopijo šolski prag.

MED INCIDENTOM:

Ko je ravnatelj seznanjen z določenim incidentom, dogodkom ali protipravnim dejanjem, se mora nemudoma odzvati in zaščititi morebitno žrtev takšnega dogodka ter o dogodku obvestiti starše. V kolikor dogodek kaže znake storitve kaznivega dejanja, naj ne odlašaja z vključitvijo policije.

V katerih primerih mora šola nujno obvestiti policijo?

Če gre za objavo ali razširjanje golih slikovnih materialov (foto ali video) učenca ali učenke, lahko potencialno govorimo o eni izmed oblik kaznivega dejanja prikazovanja, izdelave, posesti in posredovanja pornografskega gradiva ali pridobivanja oseb, mlajših od petnajst let, za spolne namene oziroma o eni izmed oblik kaznivega dejanja zlorabe osebnih podatkov. V takih primerih je treba o incidentu nemudoma obvestiti policijo. Ravno tako naj ravnatelj nemudoma vključi policijo, ko opazi oblike nasilja, groženj ali ko je zaradi incidenta neposredno ogroženo zdravje ali življenje katerekoli osebe. Glavno vodilo ravnatelja naj bo zaščita žrtve incidenta.

Če je storilec ali več storilcev incidenta znan/znanih, mora ravnatelj tudi o ravnanju storilca/storilcev nemudoma obvestiti starše. Če storilec ni znan oziroma je ali so »skriti« v skupini ali razredu, naj poskuša ravnatelj nemudoma razjasniti potek incidenta, morebitne vzroke in druge okoliščine, ki so pripeljali do njega. Ravnatelj lahko za dosego tega po obvestilu staršem učenca oziroma učence zadrži na razgovoru po pouku v zvezi z reševanjem problema. Priporočeno je, da o tem naredi zapisnik.

Pri kršitvah, ki se zgodijo z razširjanjem spornih vsebin na internetu, je ključnega pomena tudi hitrost, zato naj nedvoumno od vpletenih učencev in njihovih staršev zahteva umik spornih vsebin z interneta oziroma družabnih omrežij in hrani dokaze ali zagotovila, da je bila protipravna vsebina umaknjena. Če se protipravna vsebina nahaja na šolskih strežnikih ali računalnikih, naj jo šolske službe nemudoma odstranijo. Pred vsako odstranitvijo vsebin predlagamo, da se zavarujejo dokazi kršitve, tako da se posname slika zaslona oziroma se shranijo dnevniške datoteke (logi) na strežniku, ki razkrivajo tako aktivnost.

Učence in njihove starše lahko ravnatelj opozori tudi na kazenskopravne in civilnopravne posledice, ki lahko sledijo takemu incidentu, kot tudi na posledice za storilce na osnovi internih aktov šole.

V primeru, da je bila žrtev učitelj, naj mu ravnatelj pomaga pri odločitvi, ali bo

dogodek prijavil oziroma ali bo sprožil ustrezne pravne postopke.

Če ravnatelj meni, da pred samo kršitvijo šola ni uspela zadostno poskrbeti, da do incidenta ne bi prišlo, naj se čim prej posvetuje s pravniki, ali lahko pričakuje sodne postopke.

V kolikor vodstvo šol ni prepričano, kaj storiti v dani situaciji, naj se obrne na **Safe.si** oziroma **info@safe.si** ali pokliče **TOM TELEFON 116 111**.

PO INCIDENTU:

Predlagamo, da ravnatelj opravi ločeno razgovore z žrtvijo in storilci ter njihovimi starši. Naj presodi, v kolikšni meri bi soočenje obeh strani (tudi s starši) pozitivno vplivalo na nadaljnji razvoj in razrešitev incidenta.

V praksi se je že večkrat izkazalo, da so neposredno po takem dogodku potrebna dodatna izobraževanja o varni in odgovorni rabi interneta oziroma o tematiki, zaradi katere je nastal problem, zato naj ravnatelj premisli o vključitvi zunanje strokovnjaka in predvidi posebno izobraževanje za vpletene.

Brez omahovanja naj v skladu z internimi akti šole sproži vse disciplinske postopke oziroma druge ukrepe, ki so predvideni za tak incident.

Incident in njegova razrešitev imata lahko pozitiven vpliv na prihodnost oziroma imata preprečevalno funkcijo pri ostalih učencih⁷ kot tudi pri povzročiteljih incidenta, zato naj ravnatelj presodi, ali se naj potek in razrešitev incidenta vključno z morebitnimi sankcijami javno predstavita na šoli.



⁷ V kazenskem pravu obstajata t. i. generalna preprečitev, katere naloga je odvrščanje ljudi od kaznivih dejanj z grožnjo s kaznimi, in specialna preprečitev, katere naloga je odvrščanje obsojenega storilca od izvršitve novega kaznivega dejanja.

Učitelj

PRED INCIDENTOM:

Učitelj, ki nadzoruje učence, mora biti natančno seznanjen z internimi akti šole. Priporočljivo je, da jih natančno prebere in ozavesti, da se bo v danem trenutku, ko bo nastal problem, pravilno odzval. Pri tem so mu lahko v pomoč študije primerov, ko se v zbornici z drugimi učitelji pogovori o morebitnih primerih incidentov in o tem, kako se odzvati.

Priporočljivo je, da učitelji razredniki na razrednih urah na začetku šolskega leta s pravili seznanijo učence in jim predstavijo ukrepe ob nespoštovanju. Npr. ob nedovoljeni uporabi telefona v šoli učitelj zahteva od učenca njegovo izročitev, učenec mora telefon pred učiteljem ugasniti, učitelj pa ga spravi na varno mesto in o tem napravi zaznamek. Telefon lahko po pouku dvignejo starši učenca, kar potrdijo s podpisom ob zaznamku.

Učitelj naj bo pozoren na vedenje učencev in na morebitne konflikte, ki nastajajo v fizičnem svetu. O njih naj poroča svetovalni delavki oziroma ravnatelju, kajti problem, ki nastane v fizičnem svetu, se preslika v virtualni svet in obratno. Na tak način je možno odkriti tudi spletno nasilje, ki se dogaja prepogosto skrito očem šole, saj poteka med učenci v zaprtih družabnih omrežjih.

MED INCIDENTOM:

Ko je učitelj seznanjen z incidentom, naj o tem nemudoma obvesti ravnatelja in šolsko svetovalno službo in skupaj naj poskušajo razrešiti problem. Če je učitelj problem zaznal v prostem času izven pouka, je priporočljivo, da o tem preko e-pošte obvesti ravnatelja in svetovalno službo ter poskuša pomagati žrtvi in zavaruje dokaze kršitve. Po prihodu v šolo naslednji dan naj se zjutraj nemudoma na šoli sestane z njimi in skupaj naj se odločijo, na kakšen način bodo ukrepali. V vsakem primeru ni učiteljeva naloga, da problem pomete pod preprogo z raznimi izgovori, temveč da se na šoli odkrito soočijo s problemom in ga poskušajo razrešiti.

Učitelj je lahko v veliko primerih tudi oseba, ki se ji učenec, žrtev incidenta, zaupa. V takem primeru naj mu prisluhne in stoji ob strani. Naj presodi, kdaj in kako vključiti starše učenca. Vsekakor naj obvesti ravnatelja in se z njim posvetuje o razreševanju problema.

PO INCIDENTU:

Razredne aktivnosti so lahko neposredno po kršitvi zelo burne, še posebej, če so v spor vpleteni sošolci. Učitelj mora nujno organizirati razredno uro in strogo obsoditi nasilje ter s pomočjo različnih dinamik, študijami sorodnih primerov, igrami vlog ali s povabilom zunanje strokovnjake razrešiti in zgladiti spor.

Starši

PRED INCIDENTOM:

Starši naj se odkrito pogovarjajo in sodelujejo z otrokom. Priporočljivo je, da o varni in odgovorni rabi interneta pridobijo čim več znanja oziroma se udeležijo predavanj za starše, ki jih s tem namenom organizira šola.

Starši se morajo zavedati, da so otroci sicer res »digitalni domorodci«, ki so rojeni v svet informacijske tehnologije. Res je, da so njihove veščine uporabe informacijske tehnologije na zavidljivi ravni, a zavedanje o posledicah njihovih ravnanj je prepogosto zelo nizko.

Starši naj se seznanijo, kakšna pravila veljajo na šoli, ki jo obiskuje njihov otrok, oziroma naj se seznanijo, kakšna so pravila uporabe interneta, mobilnih naprav in kakšni so postopki ob kršitvah ter morebitne sankcije. Naj delujejo proaktivno in naj pri tem sodelujejo s šolo in naj se zavedajo, da je možno, da bodo zaradi incidenta, ki ga povzroči njihov otrok, tudi sami odškodninsko odgovarjali.

MED INCIDENTOM:

Ko so starši seznanjeni s problemom, naj ne izgubijo glave, temveč naj se poskušajo čim prej pogovoriti z otrokom, pa naj bo žrtev ali storilec. Če ne vedo, kaj storiti, naj pokličejo na TOM TELEFON (116 111) ali se obrnejo na info@safe.si.

O poteku incidenta in morebitni poti razrešitve se morajo starši pozanimati pri učiteljih in ravnatelju. Predvsem naj ne sklepajo preuranjeno izključno na osnovi izpovedi njihovih otrok.

PO INCIDENTU:

Po kršitvi naj starši spremljajo otroka in naj mu pomagajo pri vzpostavitvi razmer pred kršitvijo. Naj vložijo vse napore, da bodo morebitne sporne vsebine nemudoma umaknjene, v primeru, da je incident povzročil resne posledice ali škodo, pa naj ne odlašajo z obiskom odvetnika.

Učenec

PRED INCIDENTOM:

Učenec se mora pred incidentom zavedati, da vsako njegovo dejanje nosi določene posledice, za katere mora odgovarjati.

Na spletni strani Safe.si naj učenci natančno pregledajo nasvete s številnih področij uporabe interneta in informacijske tehnologije. V primeru, da že imajo določene probleme (npr. nekdo jim je vdrl v profil na družab-

nem omrežju), lahko rešitve poiščejo v središču za pomoč na spletni strani <http://www.safe.si>.

MED INCIDENTOM:

Najpomembnejše načelo med samim incidentom je, da žrtev ni kriva, da jo nadlegujejo, česar se mora žrtev zavedati ter kršitev čim prej zaupati odrasli osebi. Zelo pomembno je tudi to, da naj učenci ne tolerirajo spletnega nasilja, temveč naj nasilneža nemudoma prijavijo in zaščitijo žrtev.

Učenci se morajo zavedati, da ko pride do incidenta, ga bodo ravnatelj, učitelji in starši poskušali odkriti in da bo v nekem trenutku resnica prišla na dan, zato naj sodelujejo s šolo. Učenci naj se zavedajo, da na internetu res težko ostaneš anonimen.

PO INCIDENTU:

Po odkritju storilcev incidenta naj se kršitelji odkrito pokesajo in naj prevzamejo krivdo. Naj se ne skrivajo za razredom.



KAZNIVA DEJANJA NA INTERNETU

Določeni incidenti, ki se zgodijo s pomočjo ali preko interneta in informacijske tehnologije, predstavljajo takšna protipravna dejanja, ki so kot kazniva določena v Kazenskem zakoniku.⁸

Kazniva dejanja, ki se potencialno lahko storijo tudi preko interneta z informacijsko tehnologijo, so: grožnja (135. člen), mučenje (135. a člen), neupravičeno prisluškovanje in zvočno snemanje (137. člen), neupravičeno slikovno snemanje (138. člen), kršitev tajnosti občil (139. člen), nedovoljena objava zasebnih pisanj (140. člen), zloraba osebnih podatkov (143. člen), kazniva dejanja zoper čast in dobro ime, spolno nasilje (171. člen), spolni napad na osebo, mlajšo od petnajst let (173. člen), pridobivanje oseb, mlajših od petnajst let, za spolne namene (173. a člen), prikazovanje, izdelava, posest in posredovanje pornografskega gradiva (176. člen), šikaniranje na delovnem mestu (197. člen), izsiljevanje (213. člen), napad na informacijski sistem (221. člen), uporaba ponarejenega negotovinskega plačilnega sredstva (247. člen), izdaja tajnih podatkov (260. člen), javno spodbujanje sovraštva, nasilja ali nestrpnosti (297. člen) ter izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (306. člen).⁹

Namen naštevanja kaznivih dejanj je, da se vodstvo šol kakor tudi učitelji, starši in učenci zavejo, da je internet popolnoma realen svet, na katerem velja kazenski zakonik, in da se pod pretvezo skrivanja za ekranom računalnika ali mobilnega telefona lahko z navidezno nedolžnim incidentom zgodi zelo resno kaznivo dejanje.

⁸ Uradno prečiščeno besedilo Kazenskega zakonika (KZ-1) je bilo objavljeno v Uradnem listu RS, št. 54/15.

⁹ Povzeto po: Završnik, 2013. Spletno in mobilno nadlegovanje: pojem, oblike, posledice in soočanje s kazenskimi pravom.



PRIMERI ZLORAB IN REŠITEV

Predstavljamo nekaj primerov zlorab in njihovega reševanja ter napotkov, kaj bi bilo smiselno narediti.

Dijakinja Maja

Mamo dijakinje Maje je zaskrbelo, da je njena hči zasvojena z družabnim omrežjem Ask.fm¹⁰, ki ga je Maja prekomerno uporabljala, zato so ji doma to preprečili. Ask.fm je nato začela uporabljati v šoli in večino odmorov je tako preživela za računalnikom v knjižnici.

Na Ask.fm je spoznala tudi fanta. Že po zelo kratkem izmenjevanju sporočil mu je sama poslala sliko svojih golih prsi. Ko je fant sliko prejel, ji je zagrozil, da bo sliko javno objavil na internetu, če ne bo imela z njim spolnih odnosov. Maja je po določenem času povedala mami, kaj se ji je zgodilo. Predvidevali sta, da si fant ne bo upal uresničiti svoje grožnje, zato sta se odločili, da ne bosta ukrepali.

Zaradi grožnje je sicer Maja prenehala komunicirati s fantom, ki pa je nato uresničil grožnjo in na internetu javno z imenom objavil njeno razgaljeno sliko.

Ker je Maja živila v manjšem kraju, je naslednji dan po objavi ta slika zaokrožila med dijaki srednje šole, ki jo je obiskovala. Iz nje so se začeli norčevati. Ko so ti dijaki prišli domov, so sliko pokazali svojim staršem. V dobrem dnevu so sliko videli skoraj vsi krajani. Naslednji dan so mimoidoči začeli zmerjati dijakinjo, ko je šla v šolo. To niso bili le njeni vrstniki, temveč tudi odrasli in starejši prebivalci kraja.

Zaradi premočnega psihičnega pritiska je dijakinja doživela živčni zlom in so jo morali odpeljati na zdravljenje v psihiatrično kliniko. Na zdravljenju je

¹⁰ Družabno omrežje je dostopno na: <https://ask.fm/>.

ostala več kot leto dni. Zmerjanja so bili deležni tudi drugi člani družine in sokrajani so jim očitali pokvarjenost. Izločili so jih iz družbenega okolja. Tudi po daljšem času se razmere niso spremenile, zato se je družina morala preseliti na drug konec Slovenije.

Tudi po preselitvi so zaznavali težave zaradi te slike, saj je slika še vedno dostopna na internetu in so jo našli tudi sokrajani v novem okolju.

Komentar:

V tem primeru lahko govorimo o sumu storitve nekaj kaznivih dejanj, med katerimi izstopata kaznivi dejanji iz 173. a oziroma 171. člena Kazenskega zakonika (KZ-1), ki opredeljujeta pridobivanje oseb, mlajših od petnajst let, za spolne namene, če je bila dijakinja mlajša od 15 let, oziroma spolno nasilje. S samo javno objavo fotografije gre za sum storitve kaznivega dejanja zloraba osebnih podatkov (143. člen), potencialno pa lahko govorimo tudi o sumu storitve kaznivega dejanja grožnje, o kateri piše 135. člen KZ-1.

Starši dijakinje v nobenem primeru ne bi smeli problema ignorirati, ampak bi morali nemudoma vključiti v razreševanje problema tudi fantove starše oziroma šolsko svetovalko, ki pa bi morala takoj predlagati vključitev policije, ki bi z vpletenimi opravila razgovor. Po incidentu je možno, da dijakinja in njeni starši uveljavljajo odškodninski zahtevek zoper fanta oziroma njegove starše za poplačilo premoženjske (izostanek, selitev idr.) in nepremoženjske škode (duševne muke).

Lažni profili na Facebooku in zalezovanje

Na Facebooku je bilo več lažnih profilov s slikami privlačnih mladih deklet, ki so pošiljala prošnje za prijateljstvo fantom, starim od 14 do 17 let. Fantje so prošnje sprejemali, ker so jih premamile privlačne slike.

Dekleta so se s fanti začela pogovarjati preko klepeta in jih kmalu začela nagovarjati k pošiljanju fotografij. Najprej so želela videti mišice fantov. Fantje so jim pošiljali slike brez majic. V naslednjem koraku so želela slike v spodnjem perilu. V tem koraku je veliko fantov spregledalo, da gre za nekaj sumljivega, in slik niso poslali. Tisti, ki so slike poslali, so prejeli sporočilo z željo po fotografiji, na kateri so popolnoma goli.

Nekateri fantje so takšne fotografije poslali. Ko so dekleta slike prejela, so nazaj poslala sporočilo, da bi se rada srečala na zmenku. Fantje so na to pristali in se dogovorili za srečanje v popoldanskih urah v enem izmed trgovskih centrov.

V trgovskem centru pa k fantu »na zmenku« ni pristopilo dekle, temveč se mu je med čakanjem približal mlajši moški in ga vprašal, če čaka dekle. Ko je fant

potrdil, se je mlajši moški predstavil za kriminalista in dejal: »To dekle sem jaz. Zdaj me pa dobro poslušaj. Če mi ne boš poslal še več svojih golih fotografij, bom to, ki jo že imam, objavil na internetu.«

Prestrašeni fantje so odšli domov in se fotografirali goli in fotografije še naprej pošiljali izsiljevalcu. Izjema je bil en fant, ki je bil tako pogumen, da je šel sam na policijo in povedal, kaj se mu je zgodilo.

Ker je šlo za posnetke spolnih zlorab otrok in izsiljevanje, je policija takoj ukrepala. Izsiljevalcu so nastavili past in v nekaj dnevih so ga ujeli. Med preiskavo so ugotovili, da je preko lažnih profilov lovil fante in jih nato izsiljeval za fotografije, ki jih je prodajal naprej.

Komentar:

Glede na to, da je kazenski del uspešno rešen, predlagamo, da se učenci v primeru, da jim nekdo grozi, obrnejo na starše oziroma zaupanja vredno odraslo osebo, npr. šolsko svetovalko ali razrednika. Tudi šola mora učence spodbujati, da bodo težave zaupali odrasli osebi in problema ne bodo reševali sami. V kolikor so fantje utrpeli kakršnokoli nepremoženjsko škodo in jo je možno dokazati, lahko zoper storilca vložijo odškodninski zahtevek.

Lažni profili in obračunavanje s sovrstniki

Na osnovni šoli so opazili, da se je pojavilo več lažnih in očitno zlonamernih Facebook profilov učencev te šole.

Izkazalo se je, da je vse lažne profile izdelal en sam učenec, ki je v prvih dveh mesecih šolskega leta ustvaril kar 6 lažnih profilov. Sledil je pogovor z učencem in njegovimi starši, ki pa so se pri tem počutili precej nemočne, saj niso razumeli, kako je prišlo do tega, da njihov sin na tak način obračunava s sošolci, ki jih ne mara, niti kako lahko preprečijo, da bi še naprej uporabljal tak pristop k reševanju svojih težav.

Komentar:

Šola se je pravilno odzvala in nemudoma, ko je odkrila storilca, na pogovor poklicala njegove starše. V primeru, da storilca ne bi našla, bi lahko ravnatelj do prihoda staršev zadržal razred, kjer se je zgodil incident, in storilca na nek način poslušal odkriti s pogovorom.

V primeru, da je bil učenec, ki je izdelal lažne profile, že star 14 let in da so bili ustvarjeni lažni profili resničnih oseb, je učenec potencialno storilec kaznivega dejanja zlorabe osebnih podatkov, in sicer kraje identitete, ki se sicer preganja na predlog. V primeru, da so učenci oz. žrtve incidenta utrpeli/utrpele premoženjsko ali nepremoženjsko škodo (duševne muke), pa lahko njihovi starši zoper povzročitelja oziroma njegove starše naperijo odškodninski zahtevek za poplačilo škode.



Odgovorni urednik: **Marko Puschner**

Oblikovanje: **Bojan Senjur**

Ilustracije: **Designed by Freepik**

Lektoriranje: **Polona Otoničar**

Tisk: **Tiskarna Pleško d.o.o.**

Naklada: **5.000 izvodov**

Izdajatelj: **Točka osveščanja o varni rabi interneta SAFE.SI,
februar 2016**

Brezplačna publikacija

Brošura je izdana pod licenco »Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija (CC BY-NC-SA 2.5 SI)
(<http://creativecommons.org/licenses/by-nc-sa/2.5/si/>)

Dovoljeno vam je:

- reproduciranje, distribuiranje, dajanje v najem in priobčevanje dela javnosti;
- predelati delo.

Pod naslednjimi pogoji:

- Priznanje avtorstva – Pri uporabi dela morate navesti izvirnega avtorja na način, ki ga je določil izvirni avtor oz. dajalec licence.
- Nekomercialno – Tega dela ne smete uporabiti v komercialne namene.
- Deljenje pod enakimi pogoji – Če spremenite, preoblikujete ali uporabite to delo v svojem delu, lahko distribuirate predelavo dela le pod licenco, ki je enaka tej.



Safe.si
Center za varnejši Internet