Na temelju članka 58.Statuta Osnovne škole DOBRI-Split i članka 118. st. 2. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (Narodne novine br. 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 94/13, 152/14, 7/17, 68/18, 98/19, 64/20) Školski odbor Osnovne škole Dobri, Split, donio je na 10.sjednici održanoj dana 24.veljače 2022.godine

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE U ŠKOLI

Uvod

Članak 1.

S obzirom na sve veću sustavnu uporabu IKT-a u školama, potrebno je voditi računa o prijetnjama informacijskom sadržaju i IKT infrastrukturi koje mogu rezultirati različitim oblicima štete informacijskom sustavu škole (npr. gubitak informacija, nemogućnost pristupa resursima i informacijskom sadržaju, uništenje opreme i sl.). Potrebno je veliku pozornost posvetiti vidu sigurnog i odgovornog korištenja IKT-a, što je moguće postići definiranjem sigurnosne politike škole.

Pravilnik vrijedi za sve korisnike IKT infrastrukture škole. U školi je u kolovozu 2020. godine postavljena infrastruktura CARNetove mreže. Učenici, učitelji i svi školski djelatnici moraju se pridržavati uputa koje im može dati administrator sustava (e-Škole tehničar).

U osnovnoj školi Dobri e-Škole tehničarem imenovana je učiteljica informatike Tamara Mijan Šušnja.

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije dio je sigurnosne politike škole. Oblikovan je uzimajući u obzir preporuke EACEA7Eurydice mreže (http://eurydice.hr) koja analizira i pruža informacije o europskim obrazovnim sustavima, a usmjerena je na strukturu i organizaciju obrazovanja u Europi na svim razinama. Pravilnik je donesen sa svrhom:

- unaprjeđenja sigurnosti školske informatičke opreme i mreže
- jasnog i nedvosmislenog određivanja načina prihvatljivog i dopuštenog korištenja IKT resursa škole
- zaštite informacijskog sadržaja i opreme

- zaštite korisnika od različitih vrsta internetskog zlostavljanja
- promoviranja sustava i usluga koji su najprikladniji za djecu
- poticanja aktivnog sudjelovanja djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici pravilne raspodjele zadataka i odgovornosti nadležnih osoba
- propisivanja sankcija u slučaju kršenja odredbi Pravilnika

Osnovne sigurnosne odredbe

Članak 2.

Materijalni i nematerijalni resursi su:

- Korisnici IKT infrastrukture su učenici, učitelji, ostali djelatnici i povremeni korisnici (gosti).
- Računalna mreža izgrađena u sklopu projekta e-Škole i iz vlastitih sredstava, računalna oprema, stara računalna mreža i računalna oprema smatraju se IKT infrastrukturom. U školi postoje interne, javne i povjerljive informacije.
- Aplikacije koje škola koristi su e-Dnevnik, e-Matica, HUSO admin, Obračun plaća s evidencijom kadrova, Meraki (središnji sustav za upravljanje računalnom mrežom), Office 2010 i Office 2016 skup programa.

Školska oprema mora se čuvati i pažljivo koristiti. Tuđi i osobni podaci škole mogu se koristiti isključivo uz prethodno odobrenje ravnatelja škole.

S obzirom na dostupnost financija sigurnosne mjere zaštite podataka su na prosječno zadovoljavajućoj razini. Trenutno sva računala koja su na Windows operativnim sustavima posjeduju antivirusni program (odnosi se na Windows 7 i starije operativne sustave). Noviji operativni sustavi, poput Windowsa 10, posjeduju Windows Defender Security Center.

Većina mjera zaštite implementirane su kod davatelja internetskih usluga (ISP-a – CARNet). Njihovi serveri blokiraju sadržaje i stranice sumnjivog karaktera. Zaposlenici naše škole posjeduju AAI@EduHr korisnički račun pa su tako dužni koristiti e-mail koji su dobili iz AAI@EduHr sustava u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

Učiteljima i drugim djelatnicima strogo je zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i druge digitalne identitete.

Svako nepridržavanje pravila od strane zaposlenika i svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se ravnatelju škole, a sankcionirat će se temeljem važećih općih akata škole.

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u preko obrasca na mrežnoj stranici http://www.cert.hr.

Školska IKT oprema i održavanje

Članak 3.

Računalna mreža je skupina od dva ili više međusobno povezanih računala. Računala u školi povezana su bežično i žičano. Računalna mreža sastoji se od novog dijela koji je izgrađen u sklopu projekta e-Škole i starog dijela mreže. U sklopu projekta e-Škole od osnivača škole imenovan je e-tehničar koji je zadužen i plaćen za održavanje navedene mrežne infrastrukture.

Računala se bežično spajaju putem bežičnih pristupnih točaka. Pristupne točke smještene su u svakoj učionici te u najvažnijim prostorima škole.

U bežičnim pristupnim točkama postavljena su tri naziva za pristup bežičnoj mreži (SSID):

a) eduroam
b) eSkole
c) guest

a) Na eduroam mrežu spajaju se učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHr sustava. Na taj način može se identificirati i pratiti njihov promet u računalnoj mreži.
b) Na mrežu eSkole se spajaju djelatnici škole koristeći unaprijed određenu lozinku.
c) Guest mreža koristi se za spajanje vanjskih partnera i posjetitelja. Partnerima i posjetiteljima koji imaju AAI@Edu račun omogućen je pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima može se na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest otvorenog je tipa. E-Škole tehničar u Meraki dashboardu mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Određena računala u školi spojena su žičanim načinom spajanja na mrežu. To su sva računala u informatičkoj učionici te računala u uredima (ured ravnatelja, tajništva, defektologa…). Računalna mreža konfigurirana je tako da nema potrebe da se računala/korisnici autentificiraju kad se spajaju na žičanu računalnu mrežu.

Većina računala u školi posjeduje operativni sustav Windows 10 s instaliranim Office 2010, 2013 ili 2016 alatima. Na svim računalima podešeno je automatsko ažuriranje operativnog sustava i popratnih Office alata. Operativni sustavi Windows 10 imaju u sebi obrambeni sustav (Windows Defender Security Center) te također i vatrozid koji posjeduju stariji operativni sustavi do Windows XP-a. Antivirusni programi, ako se koriste, koriste se na starijim operativnim sustavima i to besplatne inačice antivirusnih programa (AVG AntiVirus Free i Avast Free Antivirus).

Trenutno u školi nema potrebe samostalnog nadziranja licenciranih programa jer svi programi koji se koriste (Windows XP, 7, 8, 8.1, 10, Office 2007, 2010, 2013, 2016) licencirani su od strane Ministarstva znanosti i obrazovanja i tvrtke Microsoft. Ministarstvo znanosti i obrazovanja izradilo je web portal Centar za preuzimanje Microsoft proizvoda. Pristup portalu imaju svi odgovorni za održavanje i instalaciju računalnih programa u školama (administratori sustava, e-tehničari). U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operativni sustavi i Office alati s pripadajućim ključevima za aktivaciju.

Na ostala računala u školi učenici ne smiju ništa instalirati bez odobrenja administratora. Ako se pojavi potreba za instaliranjem dodatnog programa, učenik se mora obavezno javiti administratoru.

Svako nepridržavanje ovih pravila ima negativan utjecaj na Školu i može rezultirati pedagoškim mjerama prema učenicima sukladno Pravilniku o kriterijima za izricanje pedagoških mjera.

Prilikom završetka rada na računalu, svi korisnici računala su dužni odjaviti se sa svojih online računa (e-dnevnik, e-mail, Teams, Office 365).

Reguliranje pristupa IKT opremi

Članak 4.

Računalnoj mreži mogu pristupiti učenici, učitelji, ostali djelatnici škole te vanjski partneri i posjetitelji.

Pristup računalnoj mreži zaštićen je na nekoliko načina. Pristup ovisi o tome tko se želi spojiti na mrežu i s kojim razlogom.

U bežičnim pristupnim točkama postavljena su tri naziva za pristup bežičnoj mreži (SSID):

a) eduroam
b) eSkole
c) guest

a) Na eduroam mrežu spajaju se učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHr sustava (802.1x with custom RADIUS enkripcija). Na taj način može se identificirati i pratiti njihov promet u računalnoj mreži.
b) Na mrežu eSkole se spajaju djelatnici škole koristeći unaprijed određenu lozinku.
c) Guest mreža koristi se za spajanje vanjskih partnera i posjetitelja (Open-password-protected with Meraki RADIUS enkripcija). Partnerima i posjetiteljima koji imaju AAI@Edu račun omogućen je pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima može se na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest otvorenog je tipa. E-Škole tehničar u Meraki dashboardu mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Svi učitelji dobili su računalo u sklopu projekta e-Škole. Učitelji i ostalo osoblje također imaju pristup računalu koje je smješteno u zbornici te informatičkoj učionici. Učitelji ne moraju tražiti posebno odobrenje za korištenje informatičke učionice.

Učenici smiju koristiti računala samo uz dopuštenje učitelja. Na nastavi Informatike učenici, ako su prethodno dobili odobrenje od učitelja za uključivanje računala, smiju pod odmorom koristiti računalo za svoje potrebe. Eventualno na kraju drugog sata (nastava Informatike održava se dva sata zaredom), ako su učenici uspješno prošli sve etape nastavnog procesa tada smiju koristiti računalo uz odobrenje učitelja (za pristup internetskim sadržajima i za zabavu). Pristup aplikacijama i internetskim sadržajima određuje isključivo učitelj.

Učenici uz odobrenje učitelja smiju koristiti svoje privatne uređaje za spajanje, ali samo uz izričito dopuštenje učitelja.

Svi učitelji koji koriste informatičku učionicu moraju se držati navedenoga:

- učionica mora ostati na kraju onako kako je i zatečena
- računala se obavezno moraju ugasiti nakon uporabe
- u slučaju da jedno od računala ne radi – kontaktirati učitelja informatike
- radna mjesta moraju ostati čista
- radno mjesto mora ostati uredno – namještena tipkovnica, miš, monitor, stolica na svom mjestu
- prozore obavezno zatvoriti
- učionicu zaključati

Učitelj informatike odgovoran je za informatičku učionicu.

Računalima u informatičkoj učionici pristupa se preko dva računa. Jedan račun koristi administrator, a drugi koriste učenici. Račun administratora zaštićen je lozinkom, dok račun za učenike nije zaštićen lozinkom.

U slučaju da bude potrebe za korištenjem korisničke zaporke u nastavku slijedi smjernica za izradu: ne smije biti kraća od 6 znakova, treba imati kombinaciju velikih i malih slova, mora imati minimalno jedan broj i jedan poseban znak.

Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNetovu mrežu automatski su uključene u sustav filtriranja nepoćudnih sadržaja.

Učenici su upoznati s informacijama o sustavu, odnosno da je sustav podešen tako da filtrira nepoćudan sadržaj, to im se posebno naglašava te se o tome educiraju na nastavi Informatike. Učenici su stalno pod nadzorom te im je u potpunosti onemogućeno zaobilaženje sigurnosnih postavki računalne opreme.

Sigurnost korisnika

Članak 5.

U školama je potrebna neprekidna edukacija učenika, učitelja i cijelog školskog kolektiva kako bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama računalnoj sigurnosti.

Korisnici računala i programa koji zahtijevaju prijavu moraju posebno paziti da prilikom prijave ne otkriju svoje podatke. Isto tako, učitelji kada odlaze iz učionice, a ostavljaju računalo uključeno, obavezno se moraju odjaviti iz svih sustava u koje su se prijavili.

Učenici, učitelji i ostali djelatnici moraju posebno voditi računa o svojem digitalnom identitetu koji su dobili iz sustava AAI@edu. Svoje podatke moraju čuvati.

Zasad je dopušteno u potpunosti preuzimanje datoteka na lokalna računala te pokretanje izvršnih datoteka. Ako vrijeme pokaže da se na taj način računala inficiraju zlonamjernim programima, e-tehničar će uvesti restrikciju na takvu vrstu interakcije.

Učenicima prestaju prava nad elektroničkim identitetom kada završe školovanje. Učiteljima i ostalom osoblju prestaju prava kada završe radni vijek, tj. odlaskom u mirovinu ili prestankom rada u školskom sustavu.

Ponašanje na internetu

Članak 6.

Svaki pojedinac odgovoran je za svoje ponašanje u virtualnom svijetu te se prema drugim korisnicima mora ponašati pristojno, ne vrijeđati ih niti objavljivati neprimjerene sadržaje.

Svakog korisnika interneta nužno je upoznati s osnovnim pravilima ponašanja u internetskoj komunikaciji i u internetskom okruženju. To se još naziva i „internetskim bontonom", a vrlo čest naziv je i „Netiquette". „Netiquette" je ustaljen popis pravila lijepog ponašanja u internetskoj komunikaciji i preveden je na mnoštvo jezika. Hrvatske stranice dostupne su na http://hr-netiquette.org. „Netiquette" propisuje smjernice i pravila ponašanja u tri (3) kategorije: elektronička pošta, popis e-adresa i forumi.

Škola je ovaj skup pravila učinila dostupnim svojim učenicima, o tome ih podučava te primjenjuje vlastitu politiku u skladu s tim pravilima.

1. Elektronička pošta
    - Ako ne koristite postupke enkripcije (*hardware* ili *software*), morate znati da elektronička pošta na internetu nije sigurna. Nemojte nikada staviti u e-mail ono što ne biste stavili na dopisnicu.
    - Poštujte vlasnička prava nad materijalima koje reproducirate. Skoro sve zemlje imaju zakone o vlasničkim pravima.
    - Ako prosljeđujete poruku koju ste primili, ne mijenjajte sadržaj. Ako je to bila osobna poruka upućena vama i vi je preusmjeravate grupi, zatražite dopuštenje. Možete je kratiti i citirati samo dijelove od značaja, ali naznačite njezinog autora.
    - Nikad ne šaljite „lance sreće" elektorničkom poštom. „Lanci sreće" su zabranjeni na internetu. Pristup mreži (ili servisu ili forumu) može vam biti uskraćen.
    - Olakšajte stvari primatelju. Mnogi programi za e-mail izbrišu podatke iz zaglavlja koji sadrže adresu za odgovor. Da biste bili sigurni da ljudi znaju tko ste, uključite liniju ili dvije na kraju poruke s podacima za kontakt. Možete napraviti datoteku s kontaktnim podacima i uključivati ga na kraj svojim poruka. Neki programi to rade automatski. U internetskom žargonu to je poznato kao .sig ili signature datoteka. Vaša .sig datoteka će nadomjestiti vašu posjetnicu, a možete ih imati nekoliko za različite prigode.

- Ukoliko uključujete signature datoteku, pazite da bude kratka. Preporučljiva duljina bilabi ne više od četiri linije. Imajte na umu da mnogi ljudi plaćaju pristup internetu po minuti i što je vaša poruka dulja, oni više plaćaju.
- Budite oprezni prilikom slanja elektroničke pošte. Postoje adrese koje predstavljaju grupu ljudi, a izgledaju kao da se radi o jednoj osobi. Znajte kome šaljete e-mail.
- Imajte na umu da je primatelj ljudsko biće, čija se kultura, jezik i smisao za humor mogurazlikovati od vaših. Problema može biti i s oblikom zapisa datuma, s mjernim jedinicama i idiomima. Budite osobito oprezni sa sarkazmom.
- Ne koristite isključivo velika slova. VELIKA SLOVA IZGLEDAJU KAO DA VIČETE.
- Koristite *smileye* da naznačite ton, ali koristite ih s mjerom. **:-)** je primjer *smileya* (nakrivite glavu). Nemojte misliti da će time primatelj nužno biti zadovoljan sadržajem poruke ili da ćete time poništiti uvredljivu poruku.
- Ne šaljite velike količine podataka ljudima koji ih nisu zatražili.

2. Mailing liste, news grupe (usenet)

Sva pravila za elektroničku poštu vrijede i ovdje.

- Čitajte mailing liste i news grupe mjesec ili dva prije nego što na njih nešto pošaljete. Ovo će vam pomoći razumjeti pravila ponašanja grupe.
- Ne okrivljujte sistem administratora zbog ponašanja korisnika sistema.
- Pretpostavite da pojedinci govore u svoje osobno ime i da ono što napišu ne predstavlja njihovu organizaciju (osim ako nije eksplicitno navedeno).
- Imajte na umu da i elektronička pošta i news troše resurse sistema. Obratite pozornost na sva pravila koja vaša organizacija može imati o korištenju ovih resursa.
- Poruke i članci trebaju biti kratki i u vezi s onim o čemu se raspravlja. Ne skrećite s teme, suvislo se izražavajte i ne šaljite poruke samo zato da biste ukazali na tuđe pogreške u tipkanju ili pravopisu. Ovakvo ponašanje će Vas, više od bilo čega, označiti kao nezrelog početnika.
- Lažno predstavljanje nije dopušteno.
- Oglašavanje je dopušteno na nekim listama i grupama, a osuđivano na drugima! Ovo je još jedan primjer zašto treba upoznati auditorij prije slanja poruke. Nezatražene reklamne poruke koje se ne tiču teme rasprave sigurno će uzrokovati da dobijete mnogo ljutitih odgovora.

- Pročitajte sve članke u slijedu (*thread*) prije nego što pošaljete odgovor. Ne šaljite „Ja također" poruke čiji sadržaj je ograničen na slaganje s prethodnom porukom. Sadržaj poruke trebao bi proširivati onu na koju se nadovezuje.
- Pošaljite odgovor elektroničkom poštom ako se tiče samo jedne osobe. *Newsi* se globalno distribuiraju i cijeli svijet vjerojatno nije zainteresiran za osobne odgovore. Nemojte, međutim, oklijevati da pošaljete nešto od interesa za sve sudionike u raspravi.
- Ako mislite da je članak od interesa za više grupa, budite sigurni da ga *crosspostate*, a ne da ga šaljete posebno u svaku grupu. Općenito, ne više od pet-šest grupa će imati interese dovoljno slične da bi se to činilo.
- Razmislite o korištenju priručnika, knjiga, help datoteka i sl. prije nego što postavite pitanje na *newsima*. Postavljanje pitanja za koje postoje odgovori na drugim mjestima imat će za posljedicu mrzovoljne „RTFM" odgovore (*read the fine manual* – iako postoji i vulgarno značenje za „F" riječ).
- Iako postoje *news* grupe u kojima je oglašavanje dopušteno, općenito se smatra kriminalnim činom oglašavati proizvode koji se ne tiču same rasprave. Ako pošaljete oglasnu poruku na mnogo grupa, vjerojatno ćete izgubiti pravo na pristup internetu!
- Predstavljanje tuđim imenom u *news* člancima nije dopušteno. Od toga se možete zaštiti korištenjem softwarea koji generira „otisak prsta" kao što je PGP.

3. Forumi

Prije svega

- Ako postoje pravila foruma, obavezno ih pročitajte i pridržavajte ih se.
- Ako postoji FAQ lista (često postavljena pitanja), obavezno je pročitajte. Možda ćete upravo tamo naći informaciju koju ste tražili.

Nazivanje i otvaranje tema

- Dobro pogledajte forum i budite sigurni da započinjete raspravu u pravom dijelu foruma.
- Prije nego li započnete temu, pretražite forum i potražite sličnu temu. Možda već postoji rasprava poput one koju namjeravate započeti.
- Iz naslova vaše teme mora biti jasno o kojoj se temi radi.
- Naslov teme mora biti kratak i jasan.

Pisanje poruka

- Pišite poruke kad imate opravdan razlog, a ona mora biti smislena.
- Nastojte da bude što jasnija i jednoznačna. Izbjegavajte nesporazume, koliko je to moguće.
- Pišite u prijateljskom tonu uz poštivanje teme.
- Prije nego li pošaljete poruku, provjerite jeste li sve napisali kako ste htjeli.
- Kada nastavljate raspravu, pročitajte sve prijašnje poruke kako biste bili sigurni da nećete dodati informaciju koja već postoji.
- Ako u vrlo staru temu dodajete novu poruku, budite sigurni da je ona vrijedna toga.
- Ne koristite isključivo velika slova. VELIKA SLOVA IZGLEDAJU KAO DA VIČETE.

Citiranje

- Kod odgovora (*reply*), citirajte poruku na koju odgovarate.
- Ukoliko je poruka na koju odgovarate dugačka, citirajte samo bitne dijelove.

Privatni razgovori

- Privatni razgovori na javnom dijelu foruma nisu poželjni. Za njih koristite privatne poruke ako postoje ili e-mail.

Potpisi

- Nastojte da vaši potpisi budu što kraći i neupadljiviji.
- Nastojte ne stavljati slike u potpise.

Učenike se poučava da ne otkrivaju osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta (na servisima poput Facebooka, Twitera, chat sobe…).

Pravila sigurnog ponašanja:

- Osobne informacije nikad se ne smiju odavati na internetu.

- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke!
- Treba pomoći prijateljima koji su zlostavljani preko interneta tako da se to ne prikriva i da se odmah obavijeste odrasli.
- Provjeriti je li Facebook profil skriven za osobe koje nam nisu „prijatelji". Treba biti kritičan prema ljudima koji se primaju za prijatelje.
- Potrebno je biti oprezan s izborom fotografija koje se objavljuju na Facebooku.
- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

Autorsko pravo

Članak 7.

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama. Creative Commons licence su skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Svaka od licenci pomaže autorima da zadrže svoja autorska prava, a drugima dopuste da umnožavaju, distribuiraju i na neke druge načine koriste njihova djela, barem u nekomercijalne svrhe. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Učitelji, učenici i ostali djelatnici se potiču da potpisuju materijale koje su sami izradili koristeći neku od licenci te da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti je dozvoljeno primati tuđe radove s interneta.

Korištenje tuđih radova s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Računalni programi su također zaštićeni zakonom kao i jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju. U to su uključeni i on-line programi odnosno web-aplikacije.

Kod mrežnih mjesta moguće je posebno zaštititi samo objavljeni sadržaj, a moguće je zaštititi i elemente koji se odnose na samo mrežno mjesto i djelo su dizajnera i/ili tvrtke/osobe koja je izradila samo mrežno mjesto.

Dijeljenje datoteka

Članak 8.

Prednost digitalnog sadržaja je da se ne uništava niti mu se umanjuje kvaliteta s brojem kopiranja. Ipak, baš zbog toga potrebno je biti vrlo oprezan s korištenjem digitalnih materijala, a još više s njihovim dijeljenjem. Naime, dijeljenje datoteka, samo po sebi, nije nelegalno. U slučaju da je datoteka proizvod pojedinca, pojedinac je može bez problema podijeliti s drugima na različite načine. Pritom je uputno zaštititi djelo nekom vrstom prikladne licence.

Primjer nelegalnog dijeljenja datoteka je kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili video sadržaja. Mnogi online servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, videosadržaja ili e-knjiga na nelegalan način. Primjer su klijenti (npr. Torrent) koji omogućuju dijeljenje sadržaja između računala pa se tako dijele najčešće nelegalno nabavljeni videosadržaji te glazbeni sadržaji, ključevi za korištenje različitih operacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, gdje je izričito zabranjeno daljnje distribuiranje i umnožavanje bez dozvole autora ili bez plaćanja naknade. Postoje i različiti oblici mrežnog servisa koji omogućuje registraciju korisnika za vrlo nisku mjesečnu pretplatu te nude preuzimanje gotovo neograničene količine digitalnog sadržaja koji je zaštićen autorskim pravom, no to je također nelegalno.

U školi se izričito zabranjuje nelegalno kopiranje ili preuzimanje autorski zaštićenog materijala. Zabranjeno je korištenje popularno zvanih torrenta.

Obaveze ustanove su:

1. Učenike i učitelje podučiti o autorskom pravu i intelektualnom vlasništvu.
2. Učenike i učitelje podučiti i usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva. Mogu se koristiti materijali sa stranice https://creativecommons.org/licenses/?lang=hr .
3. Učenike i učitelje informirati o načinima nelegalnog dijeljenja datoteka i o servisima koji to omogućuju, poput *Torrent* servisa i nekih drugih mrežnih mjesta koja zahtijevaju registraciju i plaćanje vrlo niske članarine za neograničeno preuzimanje digitalnog sadržaja i sl.
4. Učenike i učitelje informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Škola ne odgovara za podatke (gubitak, kopiranje) i zadržava pravo brisanja podataka koji se nalaze na računalu u bilo kojem trenutku i bez najave.

Nasilje na internetu

Članak 9.

Internetsko nasilje se općenito može definirati kao namjerno i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja. Nasilje preko interneta, u svijetu poznato kao *cyberbullying*, opći je pojam za svaku komunikacijsku aktivnost *cyber* tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro.

Postoje različiti oblici internetskog zlostavljanja:

- nastavljanje slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem
- *cyberbullying*
- nasilje preko mobitela
- nasilje na chatu
- nasilje na forumu
- nasilje na blogu
- nasilje na web servisima (društvene mreže)
- svi ostali oblici nasilja preko interneta
- otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima
- lažno predstavljanje žrtve na internetu
- slanje prijetećih poruka žrtvi koristeći različite internetske servise (npr. Facebook, Skype, e-mail...)
- postavljanje internetske ankete o žrtvi
- slanje virusa na e-mail ili mobitel
- slanje uznemirujućih fotografija putem e-maila, mms-a ili drugih komunikacijskih alata.

Nasilje u školama postao je sve veći problem tijekom nekoliko posljednjih godina, a budući da sve više djece koristi internet i mobilne telefone za komuniciranje, internetsko nasilje - *cyberbullying* postalo je velik problem. U nekim zemljama ovom se problemu pristupa u suradnji s udrugama ili drugim javnim tijelima koja djeluju u školama.

Iako se velika količina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanjem djece savjetniku i sl.), postoje i situacije koje zahtijevaju službenu reakciju škole. To se događa u slučajevima koji uključuju ozbiljne prijetnje prema drugim učenicima, a rezultiraju time da žrtva više

ne želi ići u školu ili pak ako se nasilje nastavi iako su već korištena druga neformalna sredstva. U takvim težim oblicima zlostavljanja potrebno je izreći neku od disciplinskih mjera škole.

Važno je istaknuti da su svi oblici nasilničkog ponašanja u školi nedopušteni i da će disciplinski odgovarati svi oni za koje se utvrdi da provode takve aktivnosti.

Edukacija o neprihvatljivom ponašanju na internetu provodi se kroz predmete koji koriste tehnologiju i na satovima razrednika, a pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva su i u prostorijama škole.

Stručna služba škole provodit će savjetodavni rad s učenicima koji prolaze ili uzrokuju manje oblike uznemiravanja, a strateški će se provoditi preventivne mjere suzbijanja nasilja.

Škola se obvezuje da će:

1. Podučiti učenike i učitelje o mogućim oblicima internetskog nasilja.
2. Podučiti učenike i učitelje o tome kako prepoznati internetsko nasilje.
3. Jasno istaknuti prihvatljiva pravila ponašanja te učenike i učitelje podučiti kroz predmete koji koriste tehnologiju.
4. Izraditi strategiju odgovora na internetsko nasilje, i to na blaži i teži oblik.
5. Razviti nultu stopu tolerancije na internetsko nasilje.
6. Obilježavati Dane sigurnog korištenja interneta i suzbijanja nasilja kroz kreativne radove (npr. natječaj za najbolji videouradak, likovni ili literarni uradak na temu internetskog nasilja kako bi se potaknula svijest o toj temi među učenicima).

Korištenje mobilnih telefona

Članak 10.

Kućnim redom škole propisano je da je zabranjeno korištenje mobitela za vrijeme nastave.

U slučaju prekršaja učitelj ima pravo oduzeti učeniku mobitel i pohraniti ga kod sebe, u tajništvu ili kod ravnatelja škole. Mobitel može preuzeti isključivo učenikov roditelj ili skrbnik.

Učenici mogu koristiti mobitel u slobodno vrijeme (mali odmor, veliki odmor) poštujući odredbe Pravilnika i Kućnog reda.

Iznimno, učenici mogu koristiti mobitele za vrijeme nastave kao nastavno pomagalo kada učitelj to zatraži i pravovremeno najavi. Svaka upotreba tehnologije u učionici mora imati unaprijed zadanu svrhu koja opravdava korištenje tehnologije. Stoga je važno da cilj svake upotrebe mobilne

tehnologije u učionici bude učenje nečeg novog ili ponavljanje poznatih stvari na nov i učenicima zanimljiv način.

Škola je dužna upoznati učenika s posljedicama zlouporabe mobitela. Jedan od popularnih oblika nasilja među vršnjacima koji donosi moderno doba tehnologije je i nasilje putem mobitela. Uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti, a može biti tekstualna, videoporuka, fotografija, poziv, odnosno bilo kakva višestruko slana poruka kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona. Škola će na roditeljskim sastancima informirati roditelje o savjetovanju učenika o korištenju mobitela:

- Naglasiti im da budu pažljivi kome daju broj mobitela.
- Neka pažljivo koriste neku od chat usluga s mobitela.
- Ako dobiju poruku s nepoznatog broja, neka ne odgovaraju.
- Ne trebaju odgovarati ni na poznate brojeve ako se zbog sadržaja poruke osjećaju loše ili neugodno.
- Objasniti djeci kako šala može lako od smiješne postati uvredljivom, i to da, ako su ljuti, mogu učiniti nešto zbog čega poslije mogu požaliti. Istaknuti im da trebaju biti pažljivi kada šalju poruke drugima
- Potaknuti ih da se prije slanja poruke zapitaju može li ona uvrijediti ili na bilo koji način naštetiti primatelju.
- Postaviti pravilo prema kojem nije dopušteno slati fotografije ili videozapise drugih ljudi bez njihova dopuštenja, kao ni slati sadržaje koji mogu uvrijediti druge ljude.

- Ako dijete dobije neprimjerenu poruku, poziv ili je izloženo nasilju, dati mu podršku i potaknuti ga da odmah razgovara s vama ili nekom drugom odraslom osobom u koju ima povjerenja (poput učitelja ili školskog psihologa) kako se problem ne bi pogoršao.
- Ako je riječ o ozbiljnijim oblicima nasilja, osobito zastrašujućim prijetnjama, razmisliti o tome da se sve prijavi policiji. U takvim slučajevima dobro je sačuvati poruke u mobitelu ili negdje drugdje zapisati podatke o datumu, vremenu i sadržaju poruke ili poziva.

Mobilni telefoni sve više imaju potpuni pristup internetu i djeca i mladi koriste fiksne internetske veze kao i mobitele za pretraživanje interneta. Stoga, iste sigurnosne mjere za korištenje interneta postaju važne i za korištenje mobilnih telefona (zaštita osobnih podataka).

Zamjenica predsjednice Školskog odbora

Bruna Ovčar

Ovaj pravilnik stupa na snagu danom donošenja te se objavljuje na mrežnom mjestu škole.

KLASA: 011-02/22-01/1

URBROJ: 2181-1-280-01-22-1

U Splitu, 24.veljače 2022.

Osnovna škola DOBRI 1 Split

Ravnateljica

Mirjana Dodig