Osnovna škola Izidora Kršnjavoga
Kršnjavoga 2
Zagreb

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OSNOVNE ŠKOLE IZIDORA KRŠNJAVOGA

Zagreb, ožujak 2018.

Na temelju članka 26. stavka 3. alineje 9. Statuta škole te odredbe članka 118. stavka 2. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 126/12, 94/13, 152/14 i 07/17) Školski odbor, a na prijedlog ravnateljice, na sjednici održanoj 13. 3. 2018. donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OSNOVNE ŠKOLE IZIDORA KRŠNJAVOGA

1. Uvod

Članak 1.

Moderan način učenja i poučavanja zahtijeva sve veću sustavnu uporabu IKT-a u školama, a samim time potrebno je voditi računa o važnosti zaštite informacijskih sadržaja i IKT infrastrukture koje mogu rezultirati različitim oblicima štete informacijskom sustavu škole (npr. gubitak informacija, nemogućnost pristupa resursima i informacijskom sadržaju, uništenje opreme i sl.). Zbog toga je potrebno veliku pozornost posvetiti obliku sigurnog i odgovornog korištenja IKT-a, što je moguće postići definiranjem sigurnosne politike škole.

Članak 2.

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

Članak 3.

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije je dio 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.

Članak 4.

Pravilnik je donesen sa svrhom:

- unaprjeđenja sigurnosti školske informatičke opreme i mreže
- jasno i nedvosmisleno odrediti načine 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

2. Osnovne sigurnosne odredbe

Članak 5.

Materijalni i nematerijalni resursi škole izravno povezani s IKT infrastrukturom. Korisnici IKT infrastrukture škole su: učenici, učitelji, ostali djelatnici škole i povremeni korisnici (gosti).

Članak 6.

Kompletna računalna mreža (žičana i bežična) izgrađena u sklopu pilot projekta e-Škole i računalna oprema dobivena kroz isti projekt, te ranije izgrađena školska računalna mreža i računalna oprema nabavljena sredstvima škole (računala, pametne ploče, LCD projektori, pisači, karaoke sustavi, sustav za nadzor, telefonska centrala, itd.) smatraju se IKT infrastrukturom.

Članak 7.

U poslovanju Škole razlikujemo javne i povjerljive informacije. Javne informacije su one koje su vezane uz djelatnost Škole i čija je javna dostupnost u interesu Škole (kontakt podaci Škole, promidžbeni materijali, internetske stranice Škole, informacije koje je Škola u skladu sa zakonom dužna objavljivati i sl.). Povjerljive informacije su osobni podaci djelatnika, učenika, (npr. kontakt podaci osobe, fotografije osobe…), podaci iz evidencija koje vodi Škola (e-Dnevnik, e-Matica, matične knjige…) te informacije koje se smatraju poslovnom tajnom. Tuđi osobni podaci mogu se koristiti isključivo uz prethodno odobrenje ravnatelja ili osobe koju on za to posebno opunomoći.

Članak 8.

Škola koristi slijedeće aplikacije: e-Dnevnik, e-Matica, HUSO admin, Centralni obračun plaća (COP), e-HZMO, e-nabava, Centralni registar Grada Zagreba, zaštićene stranice Grada Zagreba za financijsko poslovanje, Registar zaposlenih u javnom sektoru, Meraki (središnji sustav za upravljanje računalnom mrežom), Labis 8 – programski paket za uredsko poslovanje, Program za prehranu i produženi boravak, Optimus Lab online backup – programski paket za sigurnosno kopiranje podataka, Program za rad u knjižnici, SPSS - program za obradu statističkih podataka, Aplikacija za interaktivno upravljanje učionicom SAMSUNG SCHOOL, Magic Bord i StarBoard Software – aplikacije za rad s pametnim pločama, Deep Freeze, ESET NOD 32 Antivirus, Office 2010/2013/2016, OS Windows 7/8/8.1/10, Skup edukativnih programa u sklopu nastave Informatike i Tehničke kulture – Python, Easy Gif Animator, Movie Maker, Expression Web4, Bojanje, MSW Logo, QBasic; Mblock, Robopro, microbit online - programi za rad s micro: bit računalima i mBot robotima.

Članak 9.

Školska oprema se mora čuvati i pažljivo koristiti. Tuđi i osobni podaci škole i zaposlenika škole mogu se koristiti isključivo samo uz prethodno odobrenje ravnateljice škole, a preko službenika za informiranje.

Članak 10.

Sigurnosne mjere zaštite podataka u školi: Sva računala koja se koriste za uredsko poslovanje: u računovodstvu, tajništvu, ravnateljstvu, stručnoj službi, zbornici, knjižnici, Školi u bolnici, učiteljska računala, u informatičkim učionicama te računala uz pametne ekrane s funkcijom dodira zaštićena su antivirusnim programom ESET NOD 32 Antivirus (školska godišnja licenca) i Vatrozid za Windows. Sva računala u informatičkim učionicama koriste program Deep Freeze (trajna školska licenca) i Vatrozid za Windows. Sva računala u učionicama koriste Microsoft Security Essentials besplatni Microsoft-ov antivirusni program i Vatrozid za Windows. Za podatke koji se nalaze na računalima u računovodstvu, tajništvu i ravnateljstvu koristi se programski paket za sigurnosno kopiranje podataka Optimus Lab online backup tvrtke Optimus Lab d.o.o. (godišnji ugovor o isporuci i održavanju). Za učenike, učitelje i ostale djelatnike koji se spajaju na računalnu mrežu škole sa svojim privatnim računalima ili pametnim telefonima, te za uređaje dodijeljene nastavnom osoblju kroz projekt e-Škole nemamo sustavno uređeni pristup zaštite podataka na razini škole.

Članak 11.

Za sva računala u ustanovi CARNet, kao davatelju internetskih usluga, implementirao je sustav filtriranja nepoćudnih sadržaja. Odlukom MZO-a onemogućeno je prikazivanje 14 kategorija stranica s nepoćudnim i sumnjivim sadržajima. Svi 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 je strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i druge digitalne identitete. To se odnosi na pristup školskim računalima, e-Matici, e-Dnevniku, računovodstvenim programima, knjižničarskim programima i ostalim informacijskim sustavima ili mrežnim aplikacijama koje sadrže osobne podatke djelatnika i/ili učenika.

Članak 12.

Svi djelatnici škole dužni su potpisati izjavu o tajnosti podataka te se moraju pridržavati etičkih načela pri korištenju IKT-a. Svako nepridržavanje pravilima od strane zaposlenika i svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se ravnateljici škole, a sankcionirati će se temeljem važećih općih akata škole. Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u preko obrasca na mrežnoj stranici www.cert.hr .

3. Školska IKT oprema i održavanje

Članak 13.

Računalna mreža je skup povezanih računala koja omogućuje brzu razmjenu podataka neovisno o njihovoj udaljenosti. Računalnu mrežu škole čine sva stolna i prijenosna računala u učionicama, informatičkim učionicama, u zbornici, u pratećim službama, knjižnici te u Školi u bolnici i svi tableti namijenjena za rad u STEM učionicama.

Članak 14.

Računala u školi su povezana bežično i žičano. Računalna mreža se sastoji od novog dijela koje je izgrađen u sklopu e-Škole projekta te postojećeg dijela mreže koji je škola izgradila iz vlastitih sredstava. U sklopu e-Škole projekta osnivač škole (Grad Zagreb) imenovao je e-tehničara (na početku zaposlenik Gradskog ureda za obrazovanje, kasnije zaposlenik škole) koji je zadužen za održavanje navedene mrežne infrastrukture izgrađene u sklopu projekta.

Članak 15.

Obzirom da je električni i elektronički otpad (EE otpad) klasificiran kao opasni otpad, on se mora sakupljati i odvoziti odvojeno od ostalog otpada. Računalni otpad iz naše škole odvozi i zbrinjava ovlaštena tvrtka za zbrinjavanje EE otpada.

Članak 16.

Računala se bežično spajaju na 32 bežične pristupne točke u matičnoj školi i 2 bežične pristupne točke u Školi u bolnici. Pristupne točke su smještene u svakoj učionici te u najvažnijim prostorima škole (zbornica, knjižnica, polivalentna dvorana, sportska dvorana) te u dvjema Učionicama budućnosti u Školi u bolnici.

Članak 17.

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

- eduroam
- eSkole
- guest.

Članak 18.

Računala koja su spojena žičano su sva računala u informatičkim učionicama (34 računala), računala u uredima (ured ravnateljice, tajništvo, računovodstvo, zbornica, uredi pedagoga, psihologa i logopeda, knjižnica), te u klasičnim učionicama. Sveukupno 70 računala spojeno je na računalnu mrežu žičanim putem.

Članak 19.

Većina računala u školi posjeduje operativni sustav Windows 7/10 s instaliranim Office 2010/2013/2016 alatima. Postavke na računalima podešene su tako da na učeničkim računalima u informatičkim učionicama i na računalima u klasičnim učionicama postoje dva korisnička profila - administratorski, zaštićen lozinkom i učenički ili učiteljski račun koji su ograničeni i kod prijave u operativni sustav nemaju zaporke. Računala u uredima (ured ravnateljice, tajništvo, računovodstvo, zbornica, uredi pedagoga, psihologa i logopeda, knjižnica) su kod ulaza u operativni sustav zaštićeni zaporkom. Također je uključena opcija da lozinka nikada ne ističe (Password never expires).

Članak 20.

Kod svih računala je podešeno ažuriranje operativnog sustava i popratnih Office alata na automatski. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi na ažuriranje navedenog.

Članak 21.

Sva računala koja se koriste za uredsko poslovanje: u računovodstvu, tajništvu, ravnateljstvu, stručnoj službi, u zbornici, knjižnici, Školi u bolnici, profesorska računala u informatičkim učionicama te računala uz pametne ekrane s funkcijom dodira zaštićena su antivirosnim programom ESET NOD 32 Antivirus (školska godišnja licenca) i Vatrozid za Windows. Sva računala u informatičkim učionicama koriste program Deep Freeze (trajna školska licenca) i Vatrozid za Windows. Sva računala u učionicama koriste Microsoft Security Essentials besplatni Microsoft-ov antivirusni program i Vatrozid za Windows.

Članak 22.

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

Članak 23.

Programi koji se koriste za uredsko poslovanje (računovodstvo, tajništvo, knjižnica, psiholog) licencirani su za antivirusni program ESET NOD 32 Antivirus. Svake godine obnavljamo školsku godišnju licencu za 17 računala, za program Deep Freez kupljena je trajna licenca za 32 računala, a edukativni programi u sklopu nastave Informatike (Python, Easy Gif Animator, Movie Maker, Expression Web4, Bojanje, MSW Logo, QBasic, program za rad s micro.bit računalima) su uglavnom besplatni (Freeware) .

Članak 24.

Učenicima nije dozvoljeno instalirati dodatne računalne programe u informatičkoj učionici bez dozvole učitelja Informatike. Računala u informatičkoj učionici su postavljena tako da je C lokalna particija "zamrznuta" (program Deep Freeze) što znači da ako učenici nešto postave, instaliraju ili obrišu u operativnom sustavu, nakon ponovnog pokretanja sustava, sustav se vraća u prvobitno stanje.

Članak 25.

Na računalima u školi koja nisu u informatičkim učionicama učenicima nije dozvoljeno išta instalirati bez odobrenja administratora. Ako se pojavi potreba za instaliranje dodatnog programa nastavnik / učenik se mora obavezno javiti administratoru.

Članak 26.

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

4. Reguliranje pristupa IKT opremi

Članak 27.

Računalnoj mreži mogu pristupiti učenici, učitelji, ostali djelatnici škole te vanjski suradnici i posjetitelji. Pristup bežičnoj računalnoj mreži je zaštićen 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):

- eduroam,
- eSkole,
- guest.

Članak 28.

Na eduroam mrežu se spajaju nastavnici 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.

Članak 29.

eSkole mreža se koristiti za spajanje uređaja u STEM učionicama gdje se učenici i nastavnici (samo u slučaju da koriste isti uređaj) spajaju preko Captive portala koji se aktivira prilikom procesa spajanja (WPA2-PSK password-protected with custom RADIUS enkripcija).

Članak 30.

Guest mreža se koristi 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 suradnicima i posjetiteljima može se na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest otvorenog je tipa, a za autentifikaciju koristi se tzv. captive portal. Kako bi im se omogućio pristup, tehničar e-Škole u Meraki sustavu mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Članak 31.

Svi su nastavnici dobili računalo u sklopu projekta e-Škole. Nastavnici iz STEM područja dobili su hibridno računalo, ravnateljica i stručne suradnice te djelatnice Škole u bolnici dobile su prijenosno računalo, a ostali nastavnici tablete. STEM učionice opremljene su tabletima koji učenici mogu koristiti samo uz odobrenje učitelja. 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.

Članak 32.

Učenici smiju koristiti računala samo uz dopuštenje nastavnika. Na nastavi Informatike učenici, ako su prethodno dobili odobrenje od nastavnika 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 nastavnika (za pristup internetskim sadržajima i za zabavu). U STEM učionicama učenici također smiju koristiti računalnu opremu samo uz odobrenje nastavnika. Pristup aplikacijama i internetskim sadržajima određuje isključivo nastavnik. Učenici smiju koristiti svoje privatne uređaje za spajanje, ali samo uz izričito dopuštenje učitelja.

Članak 33.

Svi učitelji koji koriste informatičku učionicu dužni su pridržavati navedenog:

- 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 nastavnika Informatike
- radna mjesta moraju ostati čista
- radno mjesto mora ostati uredno – namještena tipkovnica, miš, monitor, stolica na svojem mjestu
- prozore obavezno zatvoriti
- učionicu zaključati

Učitelj Informatike odgovoran je za informatičku učionicu.

Članak 34.

Postavke na računalima podešene su tako da na učeničkim računalima u informatičkim učionicama i na računalima u klasičnim učionicama postoje dva korisnička profila - administratorski, zaštićen lozinkom i učenički ili učiteljski račun koji su ograničeni i kod prijave

u operativni sustav nema zaporke. Računala u uredima (ured ravnateljice, tajništvo, računovodstvo, zbornica, uredi pedagoga, psihologa i logopeda, knjižnica) su kod ulaza u operativni sustav zaštićeni zaporkom. Također je uključena opcija u operativnom sustavu da lozinka nikada ne prestaje (Password never expires).

Članak 35.

U slučaju potrebe za korisničkom zaporkom slijediti smjernica za izradu: ne smije biti kraća od šest (6) znakova, treba imati kombinaciju velikih i malih slova, mora imati minimalno jedan broj i jedan poseban znak.

Članak 36.

Pravila za korištenje IKT opreme
Odlukom Ministarstva znanosti i obrazovanja prema kojoj se 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 istome educiraju i upućuju na nastavi Informatike. Učenici su stalno pod nadzorom te im je u potpunosti onemogućeno zaobilaženje sigurnosnih postavki računalne opreme. U školi postoji nadzor mrežnog prometa kroz Meraki Cloud System od strane e-tehničara škole.

5. Sigurnost korisnika

Članak 37.

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

Članak 38.

Kod prijave na računalima i u aplikacijama koji zahtijevaju autentifikaciju, svi korisnici dužni su posebno voditi računa da ne otkriju svoje pristupne podatke. Isto tako kada učitelji odlaze iz učionice, a ostavljaju računalo uključeno dužni su se odjaviti iz svih sustava u koje su se prijavili. Ukoliko učenici koriste računala u STEM učionicama nakon završetka rada obavezno se moraju odjaviti iz sustava u koji su se prijavili.

Članak 39.

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

Samo administratorskom računu dopušteno je u potpunosti preuzimanje datoteka na lokalna računala te pokretanje izvršnih datoteka. Učenički i učiteljski računi su ograničeni pa takva vrsta interakcije nije dozvoljena.

Članak 40.

Svi učenici, učitelji te ostalo osoblje posjeduju elektronički identitet u sustavu AAI@Edu.hr. Na početku svake godine izvodi se ponovna evidencija korisničkih računa – radi se sinkronizacija s e-maticom. Na taj način automatski se u HUSO sustav upisuju svi novi učenici. Svi učenici dobivaju elektronički identitet ispisan u analognom obliku te im se daje na čuvanje i korištenje. U slučaju da izgube svoj korisnički račun, učenik ili roditelj dolazi u tajništvo škole gdje tajnik škole (koji je i administrator imenika) ispisuje korisnički račun s novom ili po zahtjevu starom lozinkom. U slučaju da učenik seli iz naše škole u neku drugu školu, njegov elektronički identitet se privremeno briše. U slučaju da učenik iz neke škole dolazi u našu školu njegov elektronički identitet se prenosi (migrira) u našu školu. Isto vrijedi i za nastavnike i ostalo osoblje.

Članak 41.

Učenicima prestaju prava nad elektroničkim identitetom kada završe sa svojim školovanjem. Nastavnicima i ostalom osoblju prestaju prava kada završe sa svojim radnim vijekom tj. odlaskom u mirovinu ili prestankom rada u školskom sustavu.

6. Ponašanje na internetu

Članak 42.

Svaki pojedinac je odgovoran za svoje ponašanje na internetu, pa se prema drugim korisnicima mora ponašati u skladu s opće prihvaćenim pravilima pristojnog ponašanja. Nije dozvoljeno druge korisnike vrijeđati, niti objavljivati neprimjerene sadržaje. Svakog korisnika koji se susreće s internetom potrebno je upoznati s osnovnim pravilima ponašanja u takvoj komunikaciji i takvom okruženju. Ta se pravila još zovu „internetskim bontonom", a vrlo čest naziv je i 'Netiquette'. To je ustaljen popis pravila lijepog ponašanja u internetskoj komunikaciji i preveden je na mnogo jezika. Hrvatske stranice dostupne su na poveznici http://hr-netiquette.org.

Članak 43.

Naša škola je ova pravila prihvatila i primjenjuje ih u skladu s vlastitom politikom. Isto tako učenike naše škole podučavamo o ovim pravilima na nastavi, a dostupna su im i na mrežnim stranicama škole. Učenike podučavamo, da ne otkrivaju svoje osobne podatke, kao što su: adresa, ime škole, telefonske brojeve i slične podatke. Pravila ponašanja koja proizlaze iz 'Netiquette-a' možemo promatrati kroz tri oblika - elektronička pošta, popis e-adresa i forumi.

Članak 44.

a) ELEKTRONIČKA POŠTA:

- *Nesigurnost elektroničke pošte*: Ako ne koristite metode zaštite, morate znati da elektronička pošta na internetu nije sigurna i da u nju nikad ne stavljate nikakve podatke koje ne biste mogli napisati na razglednicu.
- *Poštivanje autorskih prava:* Poštujte prava vlasnika nad materijalima koje koristite jer sve zemlje imaju zakone o vlasničkim pravima.
- *Prosljeđivanje poruka*: Ako prosljeđujete poruku koju ste primili, ne mijenjajte sadržaj, zatražite dopuštenje autora ako je prosljeđujete grupi ljudi. Ukoliko iz izvorne poruke vadite njezine dijelove i šaljete drugima, onda navedite autora izvornog teksta.
- *Lanci sreće:* Nikad ne šaljite „lance sreće" elektroničkom poštom. „Lanci sreće" su zabranjeni na Internetu. Sudjelovanjem, može vam biti uskraćen pristup mreži.
- *Adresa pošiljatelja:* Mnogi programi za elektroničku poštu izbrišu podatke iz zaglavlja koji sadrže adresu za odgovor. Kako bi primatelj znao tko ste, na kraju poruke napišite svoje kontakt podatke. Možete napraviti datoteku s kontaktnim podacima i uključivati ga na kraj vaših poruka (tj. datoteke s nastavkom .sig, odnosno signature datoteke), kako bi nadomjestile vašu posjetnicu. Takva datoteka treba biti kratka (ne više od četiri retka) jer neki primatelji plaćaju pristup Internetu po minuti i što je poruka dulja, oni više plaćaju.
- *Primatelj pošte:* Obratite pozornost kome šaljete elektroničku poštu. Postoje adrese koje predstavljaju grupu ljudi, a izgledaju kao da se radi o jednoj osobi.
- *Sadržaj i smisao pošte (tekst poruke)*: Primatelj/i vaše pošte mogu biti ljudi različitog jezika, kulture, stavova i smisla za humor, zato budite oprezni s pisanjem datuma, mjernih jedinica, idioma, a posebno korištenjem humora ili sarkazma u tekstu.
- *Poštivanje pravopisa:* Poštivanje pravopisnih pravila vrijedi i za elektroničku poštu. Uz to ne koristite isključivo velika slova, jer velika slova izgledaju kao da vičete. Koristite emotikone da naznačite osjećaje, ali koristite ih s mjerom.
- *Troškovi elektroničke pošte:* Troškove elektroničke pošte snose i pošiljatelj i primatelj (ili njihove organizacije). Primatelj može imati troškove kao što su širina internet veze (bandwith), diskovni prostor ili korištenje procesora. To je ekonomski razlog zašto je oglašavanje putem elektroničke pošte ponekad neželjeno i u nekim slučajevima zabranjeno.
- *Veličina teksta:* Tekst poruke mora biti kratak i jasan jer prevelika količina teksta (podataka) može izazvati nelagodu kod primatelja. Općenito, elektronička komunikacija postoji zbog brzine slanja poruke te isticanja najvažnijeg u poruci. Isto tako, ako šaljete prevelike datoteke, postoji mogućnost da iste neće biti poslane zbog prevelike količine podataka.

Članak 45.

b) POPIS E-ADRESA (mailing liste, news grupe)

- Čitajte poruke u mailing listi i news grupi nekoliko mjeseci prije nego što na njih nešto pošaljete. To će vam pomoći razumjeti pravila ponašanja grupe.
- Za neodgovorno ponašanje korisnika, nemojte kriviti sistem administratora.
- Pretpostavlja se da pojedinci govore u svoje osobno ime i ono što napišu ne predstavlja organizaciju ili instituciju u kojoj rade (osim ako nije eksplicitno navedeno).
- Znajte da elektronička pošta i news grupe troše resurse sustava. Pazite na sva pravila koja vaša organizacija ili institucija ima o korištenju tih 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 ispravljajte tuđe pogreške.
- U elektroničkoj komunikaciji lažno predstavljanje nije dopušteno.
- Oglašavanje je dopušteno na nekim listama i grupama, a osuđivano na drugima. Zato je važno da upoznate sudionike liste ili grupe prije slanja poruke. Neželjene reklamne poruke, koje se ne tiču teme rasprave, sigurno će uzrokovati nezadovoljstvo ostalih sudionika ili ćete izgubiti pravo pristupa internetu.
- Ako sudjelujete u raspravi, pročitajte sve članke u nizu (thread) prije nego pošaljete odgovor. Sadržaj vaše poruke, treba proširivati onu na koju se nadovezuje. Ne šaljite poruke: „Ja također".
- Poruku koja se tiče samo jedne osobe, šaljite elektroničkom poštom. News-e koristite samo kada imate informacije korisne sudionicima u raspravi. Ako mislite da je članak zanimljiv većem broju grupa koristite crosspostate i ne šaljite ga svakoj grupi posebno.
- Prije postavljanja pitanja na newsima koristite priručnike, knjige, datoteke za pomoć i sl. jer odgovor na vaša pitanja možda već postoje na drugim mjestima.
- U news člancima nije dopušteno lažno se predstavljati. Od toga se možete zaštititi korištenjem programa koji generira "otisak prsta" (PGP).

Članak 46.

c) FORUMI

- Ako postoje pravila foruma, obavezno ih pročitajte i pridržavajte ih se.
- Ako postoji popis često postavljanih pitanja (FAQ - Frequently Asked Questions), obavezno ga pročitajte. Možda ćete upravo tamo naći informaciju koju tražite.
- Dobro pregledajte 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.
- Naslov teme mora biti kratak i jasan. Odnosno, iz naslova mora biti jasno o kojoj se temi radi.
- Razmislite i pažljivo sročite svoju poruku prije nego je objavite. Nastojte da vaša poruka bude jasna i smislena.
- Pišite u prijateljskom tonu i izbjegavajte nesporazume, koliko je to moguće.
- Kada nastavljate raspravu, pročitajte sve prijašnje poruke kako bi 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.
- Kod odgovora (reply), citirajte poruku na koju odgovarate.
- Ako je poruka na koju odgovarate dugačka, citirajte samo bitne dijelove.
- Privatni razgovori na javnom dijelu foruma nisu poželjni. Za njih koristite privatne poruke, ukoliko postoje, ili e-mail.
- Nastojite da vaši potpisi budu što kraći i neupadljivi.
- Nastojite ne stavljati slike u potpise. Učenike se poučava kroz nastavu Informatike i satova razrednika da ne otkrivaju osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta (na servisima popu Facebooka, Twitera, chat sobe...).

Članak 47.

d) PRAVILA SIGURNOG PONAŠANJA:

- Osobne informacije na internetu se nikad ne smiju odavati.
- 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 sakriva nego da se odmah obavijeste odrasli.
- Provjeriti je li Facebook profil skriven za osobe koji nam nisu „prijatelji". Treba biti oprezan 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*).

7. Autorsko pravo

Članak 48.

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (više na : https://creativecommons.org/licenses/?lang=hr). Creative Commons licence jesu 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.

Članak 49.

Nastavnici, učenici i ostali djelatnici potiču se da potpisuju materijale koji su sami izradili koristeći neku licencu, te da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti je dozvoljeno preuzimati tuđe radove s interneta. Korištenje tuđih radova s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Članak 50.

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 naravno 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.

8. Dijeljenje datoteka

Članak 51.

Prednost digitalnog sadržaja je da se ne uništava i ne 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 nezakonito. U

slučaju da je datoteka proizvod pojedinca, pojedinac je može bez problema podijeliti s drugima na različite načine. Pritom je, dakako, dobro zaštititi djelo nekom vrstom prikladne licence.

Članak 52.

Primjer nezakonitog dijeljenja datoteke je kopiranje ili preuzimanje autorski zaštićenoga materijala poput e-knjige, glazbe ili pak video-sadržaja. Mnogi on-line servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, video-sadržaja ili pak e-knjiga na nezakonit način. Primjer su klijenti (npr. Torrent) koji omogućuju dijeljenje sadržaja između računala pa se tako dijele najčešće nezakonito nabavljeni video sadržaji te glazbeni sadržaji, ključevi za korištenje različitih aplikacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, gdje je izričito zabranjeno daljnje distribuiranje i umnožavanje bez dozvole autora ili bez plaćanja naknade.

Članak 53.

Postoje i različiti oblici mrežnih servisa koji omogućuju registraciju korisnika za vrlo nisku mjesečnu pretplatu, te nude preuzimanje gotovo neograničenih količina digitalnog sadržaja koji je zaštićen autorskim pravom, no to je također nezakonito. U školi se izričito zabranjuje nezakonito kopiranje ili preuzimanje autorski zaštićenog materijala. Računalna mreža je postavljena tako da u potpunosti onemogućava "peer to peer" (P2P) protokole i filtrira mrežne stranice koje sadrže P2P datoteke. U potpunosti je onemogućeno korištenje popularno zvanih torrenata. Torrent klijenti moći će instalirati i pokrenuti, ali neće moći ostvariti nikakav mrežni promet.

Članak 54.

Obaveze ustanove su:

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

9. Internetsko nasilje

Članak 55.

Internetsko nasilje općenito se može definirati kao često i namjerno 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.

Članak 56.

Postoje različiti oblici internetskog zlostavljanja:

- nastavljanje slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem - Cyberbullying
- Nasilje mobitelom
- 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 (poput Facebooka, Skypea, e-maila i drugih servisa za komunikaciju)
- postavljanje internetske ankete o žrtvi
- slanje virusa na e-mail ili mobitel
- slanje uznemirujućih fotografija putem e-maila, mms-a ili drugih komunikacijskih alata.

Članak 57.

Nasilje u školama postaje 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.

Članak 58.

U nekim zemljama ovom se problemu pristupa u suradnji s udrugama ili drugim javnim tijelima koja djeluju u školama. Iako se velika većina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanja djece savjetniku i sl.), postoje i situacije kad se zahtijeva službena reakcija 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.

Članak 59.

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

Članak 60.

Edukacija o neprihvatljivom ponašanju provode se kroz predmete koji koriste tehnologiju ili Sat razrednika te su pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva i u prostorijama škole. Stručna služba škole provodit će savjetodavni rad s učenicima koji prolaze ili uzrokuju male oblike uznemiravanja, a kroz strategiju će se provesti i preventivne mjere suzbijanja nasilja. Škola se obvezuje da će:

1. Podučiti učenike i nastavnike o mogućim oblicima internetskog nasilja.

2. Učenike i nastavnike podučiti o tome kako prepoznati internetsko nasilje.
3. Jasno istaknuti prihvatljiva pravila ponašanja te učenike i nastavnike 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 među učenicima potaknula svijest o temi).

10. Korištenje mobilnih telefona

Članak 61.

Kućnim redom škole propisano je i zabranjeno korištenje mobitela za vrijeme nastave. U slučaju prekršaja nastavnik ima pravo oduzeti učeniku mobitel i pohraniti ga kod sebe, u tajništvu ili kod ravnatelja škole. Mobitel može preuzeti isključivo učenikov roditelj ili skrbnik.

Članak 62.

Učenici mogu koristiti mobitel u slobodno vrijeme (mali i veliki odmor) poštujući odredbe Pravilnika i Kućnog reda. Iznimno, učenici mogu koristiti mobitele (smartphone) za vrijeme nastave kao nastavno pomagalo kada nastavnik to zatraži i pravovremeno najavi. Svaka upotreba tehnologije u učionici mora imati unaprijed zadanu svrhu, koja opravdava korištenje tehnologije. Stoga je važno da cilj upotrebe svake mobilne tehnologije u učionici bude učenje nečeg novog ili ponavljanje poznatih činjenica na nov i učenicima zanimljiv način.

Članak 63.

Škola je dužna upoznati učenika s posljedicama zlouporabe mobitela.

Članak 64.

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 – može biti tekstualna, videoporuka, fotografija, poziv – odnosno bilo kakva višestruko slana poruka kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Članak 65.

Škola će kroz roditeljske sastanke informirati roditelje o savjetovanju učenika o korištenju mobitela:

- Naglasiti im da budu pažljivi kome daju broj mobitela.
- Neka pažljivo koriste neku od chat usluga preko 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.
- Istaknite im da budu pažljivi kad šalju poruke drugima.
- Potaknite ih da se prije slanja poruke zapitaju može li ona uvrijediti ili na bilo koji način naštetiti primatelju?
- Postavite 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, dajte mu podršku i potaknite ga da odmah razgovara s vama ili nekom drugom odraslom osobom u koju ima povjerenja (poput nastavnika, školskog psihologa) kako se problem ne bi pogoršao.
- Ako je riječ o ozbiljnijim oblicima nasilja, osobito zastrašujućim prijetnjama, razmislite o tome da sve prijavite policiji.
- U takvim slučajevima dobro je sačuvati poruke u mobitelu, ili negdje drugdje zapisati podatke o datumu, vremenu i sadržaju poruke ili poziva.

Članak 66.

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, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama, i slično)

Ovaj Pravilnik stupa na snagu danom donošenja.

KLASA: 003-05/18-02/01
URBROJ: 251-124-02-18-02
Zagreb, 13. ožujka 2018.

PREDSJEDNIK ŠKOLSKOG ODBORA

Zoran Bahtijarević, dr. med.