Srednja škola Bartola Kašića Grubišno Polje
Bartola Kašića 1, Grubišno Polje

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE SREDNJE ŠKOLE BARTOLA KAŠIĆA GRUBIŠNO POLJE

Grubišno Polje, srpanj 2018.

Na temelju članka 27. Statuta Srednje škole Bartola Kašića Grubišno Polje, 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, 94/13, 152/14 i 07/17) Školski odbor, na prijedlog ravnateljice, na sjednici održanoj 10. srpnja 2018. donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE SREDNJE ŠKOLE BARTOLA KAŠIĆA GRUBIŠNO POLJE

I. Uvod

Članak 1.

S obzirom na sve veću sustavnu upotrebu informacijsko-komunikacijekse tehnologije (u daljnjem tekstu IKT) 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.). Zbog toga je potrebno posvetiti veliku pozornost oblicima sigurnog i odgovornog korištenja IKT-a što je moguće postići definiranjem sigurnosne politike škole.

Članak 2.

Pravilnik vrijedi za sve korisnike IKT strukture Škole. U Školi je u srpnju 2017. godine postavljena infrastruktura CARNetove mreže. Učenici se trebaju pridržavati uputa navedenih u ovom Pravilniku i uputa koje im mogu dati nastavnici, djelatnici Škole i e-Škole tehničar, a kojima je cilj unapređenje sigurnosti školske informatičke opreme i mreže.

Članak 3.

Pravilnik je donesen sa svrhom:

- unapređenja 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 učenike
- poticanja aktivnog sudjelovanja učenika u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici
- pravilne raspodjele zadataka i odgovornosti nadležnih osoba
- propisivanje sankcija u slučaju kršenja odredbi Pravilnika

II. Osnovne sigurnosne odredbe

Članak 4.

Korisnici IKT infrastrukture u Školi su učenici, nastavnici, ostali djelatnici i povremeni korisnici (gosti).

IKT infrastrukturom u Školi smatraju se:

Materijalni resursi:

- Kompletna računalna mreža izgrađena u sklopu projekta e-Škole i računalna oprema dobivena kroz projekt
- Stara računalna mreža i računalna oprema (računala, pametne ploče, LCD projektori, pisači, LCD televizori, fotokopirni uređaji)

Nematerijalni resursi:

- e-dnevnik, e-matica, e-porezna, e-mirovinsko, e-zdravstveno, COP, Infomare – licenca winGPS za rad u Riznici BBŽ i Registar zaposlenih u javnom sektoru, ISGE, Metl win, e-kvaliteta, e-naukovanje, aplikacije za rad s pametnim pločama, antivirusni programi, skup edukacijskih programa u sklopu nastave Informatike, Računalstva i Računarstva, skup edukacijskih programa za stručne predmete za program Tehničar za računalstvo.

U poslovanju Škole razlikujemo javne i povjerljive informacije. Javne su one informacije koje su vezane uz djelatnost Škole i čija je javna dostupnost u interesu Škole (kontakt podatci Škole, promidžbeni materijali, internetska stranica Škole, informacije koje je Škola u skladu sa zakonom dužna objavljivati i sl.).

Povjerljive informacije osobni su podatci djelatnika, učenika (npr. kontakt podatci osobe, fotografije osobe, …), podatci iz evidencija koje vodi Škola (e-Dnevnik, e-Matica, matične knjige, …) te informacije koje se smatraju poslovnom tajnom.

Članak 5.

Svi korisnici trebaju čuvati i pažljivo upotrebljavati školsku IKT infrastrukturu, a tuđi i osobni podaci Škole i zaposlenika Škole se mogu koristiti isključivo uz prethodno odobrenje ravnatelja ili osobe koju on za to posebno opunomoći.

Sigurnosne mjere zaštite podataka u školi: sva računala zaštićena su vatrozidom za Windows i antivirusnim programima.

Za sva računala u školi CARNet kao davatelj internetskih usluga, implementirao je sustav filtriranja nepoćudnih sadržaja. Odlukom MZO-a onemogućeno je prikazivanje 14 kategorija stranica s nepoćudnim i sumnjivim sadržajima.

Učenici, nastavnici i ostali djelatnici koji se spajaju na računalnu mrežu vlastitim pametnim telefonima čiji su sustavi Android, Windows i iOS, nemaju zaštitu od strane Škole.

Osobni podatci učenika i djelatnika redovito se upotrebljavaju za poslovanje Škole dok je potrebno prethodno odobrenje ravnateljice za njihovo korištenje za one svrhe koje nisu izričito propisane nekim zakonom.

Škola ima vlastitu e-mail adresu ured@ss-bkasica-grubisnopolje.skole.hr kojom se kao ustanova koristi za komunikaciju s nadležnim tijelima i drugim institucijama.

Djelatnici Škole posjeduju AAI@EduHr korisnički račun pa su se tako dužni koristiti službenom e-mail adresom (ime.prezime@skole.hr) za službenu komunikaciju s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

Svim djelatnicima Škole strogo je zabranjeno davati učenicima vlastite zaporke i digitalne identitete.

Svi djelatnici Škole moraju se voditi načelima o tajnosti podataka i trebaju se pridržavati etičkih načela pri korištenju IKT-a.

Svako nepridržavanje pravila od strane djelatnika 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 www.cert.hr.

III. Školska IKT oprema i održavanje

Članak 6.

U Školi se nalazi optička mrežna infrastruktura koja omogućuje bežičnu povezanost u svim prostorijama Škole, a u informatičkim učionicama i žičanu povezanost.

Postoje 3 mreže (SSID):

- eduroam
- e-Skole
- guest

Za povezivanje na eduroam i e-skole mreže potrebno je posjedovati Carnetov mail *skole.hr* i pripadajuću lozinku dok je guest mreža otvorenog tipa. Za mrežu je odgovoran Carnet, a za održavanje e-škole tehničar.

Škola ima uređenu mrežnu infrastrukturu u vidu bežične povezanosti na području cijele škole. U cijeloj školi postavljeni su uređaji pristupnih točaka (Access Point) koji dijele signal bežične mreže u svakoj prostoriji škole.

Računala u prvoj informatičkoj učionici povezana su žičanom lokalnom mrežom, a u drugoj informatičkoj učionici povezana su bežičnom lokalnom mrežom. Ostala računala, tableti i

hibridna računala povezuju se bežičnom vezom. Računala u upravnoj zgradi povezana su žičanom lokalnom mrežom, ali moguće ih je povezati i bežičnom mrežom.

Članak 7.

Škola ima 2 informatičke učionice sa stolnim računalima. Na računalima su instalirane pripadajuće programske podrške. U upravnoj zgradi nalazi se 5 stolnih računala s pripadajućom programskom podrškom. Za održavanje ovih računala odgovorni su informatičari u školi (nastavnici Informatike i Računalstva).

Škola ima 2 učionice s interaktivnom pločom gdje se u jednoj od njih nalazi ormar s 30 učeničkih tableta s tipkovnicom. Nastavnici posjeduju nastavničke tablete ili hibridno računalo. Za održavanje ove opreme nadležan je e-Škole tehničar.

Sva računala u Školi posjeduju operacijski sustav Windows s instaliranim Office alatima i antivirusne programe. Na svim računalima, osim nastavničkih tableta i hibridnih računala, postavljeni su administratorski i klijentski račun osiguran lozinkom. Nastavnički tableti i hibridna računala imaju samo administratorski račun osiguran lozinkom. Na računalima u upravnoj zgradi nalazi se administratorski račun osiguran lozinkom.

U Školi nema potrebe za samostalno nadziranja licenciranih programa jer svi programi koji se upotrebljavaju licencirani su od strane Ministarstva znanosti i obrazovanja koje potpisuje ugovore s Microsoftom i ostalim tvrtkama. Ministarstvo znanosti i obrazovanja izradilo je web portal Centar za preuzimanje Microsoft proizvoda. Portalu mogu pristupiti administrator resursa, informatičari u školi, ali i e-Škole tehničar po potrebi.. U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operacijski sustavi i office alati s pripadajućim ključevima za aktivaciju.

Članak 8.

Učenicima nije dozvoljena instalacija programske podrške. Ukoliko se pojavi potreba za instaliranjem dodatnog računalnog programa, djelatnik, odnosno učenik koji ga želi instalirati dužan je obvezno se javiti nastavnicima Informatike/Računalstva ili administratoru resursa.

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

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

IV. Reguliranje pristupa IKT opremi

Članak 9.

Žičanoj i bežičnoj mrežnoj infrastrukturi mogu pristupiti učenici, nastavnici, ostali djelatnici Škole te vanjski suradnici i posjetitelji. Pristup računalnoj mreži zaštićen je na nekoliko načina.

Pristup ovisi o tome tko se želi spojiti na mrežu i s kojim razlogom. Administraciji same mreže može pristupiti e-Škole tehničar i CARNet. U bežičnim pristupnim točkama postavljena su tri naziva za pristup bežičnoj mreži (SSID):

a) eduroam
b) e-Skole
c) guest

a) Na eduroam mrežu spajaju se nastavnici i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podatcima iz AAI@EduHr sustava (802.1x with custom RADIUS enkripcija). Na taj način može se identificirati i pratiti njihov promet u računalnoj mreži.
b) e-Skole mreža upotrebljava se za spajanje uređaja u STEM učionicama gdje se učenici i nastavnici (samo u slučaju da se koriste istim uređajem) spajaju preko Captive portala koji se aktivira prilikom procesa spajanja (WPA2-PSK password-protected with custom RADIUS enkripcija).
c) Guest mreža upotrebljava se za spajanje vanjskih suradnika i posjetitelja (Open-password-protected with Meraki RADIUS enkripcija). Suradnicima i posjetiteljima koji imaju AAI@EduHr 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 otvorenoga je tipa, a za pristup se koristi captive portalom. Kako bi im se omogućio pristup, e- Škole tehničar treba u Meraki sustavu kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Članak 10.

Svi nastavnici na korištenje imaju tablet računalo u sklopu projekta e-Škole dok nastavnici iz STEM područja upotrebljavaju hibridno računalo, a ravnatelj i stručni suradnici prijenosno računalo. Jedna STEM učionica opremljena je tabletima koje učenici mogu upotrebljavati samo uz odobrenje nastavnika. Nastavnici i ostali djelatnici imaju pristup računalima u zbornici i informatičkoj učionici. Nastavnici ne moraju tražiti posebno odobrenje za korištenje informatičke učionice.

Članak 11.

Učenici smiju upotrebljavati samo školska računala koja su njima namijenjena (informatičke i STEM učionice, školska knjižnica) i to isključivo za potrebe nastave.

Vlastita računala i pametne telefone učenici smiju za vrijeme nastave upotrebljavati isključivo u obrazovne svrhe i uz prethodno dopuštenje nastavnika, pri čemu moraju paziti da ne ugrožavaju druge korisnike školske mreže širenjem virusa i drugih zlonamjernih programa. Kojim aplikacijama i internetskim sadržajima mogu pristupiti određuje nastavnik.

Učenici smiju upotrebljavati vlastita računala u privatne svrhe isključivo za vrijeme odmora te prije i poslije nastave.

Članak 12.

Svi nastavnici koji se koriste informatičkom učionicom dužni su pridržavati sljedećeg:

- učionica na kraju nastavnog sata mora ostati uredna
- 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 obvezno zatvoriti
- učionicu zaključati

Svi nastavnici koji imaju nastavu u učionici informatike odgovorni su za urednost učionice i sigurnost opreme.

Članak 13.

Na računalima u informatičkim učionicama definirana su 2 računa: administratorski i klijentski račun. Klijentski račun namijenjen je za učenike jer onemogućava instaliranje i mijenjanje programske podrške na računalu. Ažuriranje se provodi automatski kada postane dostupno ono se instalira na računala. Na računalima su instalirani antivirusni programi te su uključeni i vatrozidi.

Isti mehanizmi zaštite su i na ostalim računalima, tabletima i hibridnim računalima, s razlikom da jedino nastavnička oprema ima samo administratorski račun osiguran lozinkom. Svaki nastavnik ima svoj nastavnički tablet kojem pristupa putem lozinke i upotrebljava ga. Na mrežu se spajaju preko AAI@Edu.hr identiteta.

Administrativni djelatnici Škole (ravnateljica, pedagog, knjižničarka, računovodstvene djelatnice, tajnica) upotrebljavaju stolna računala u uredima upravne zgrade koja su zaštićena lozinkom i imaju adminstratorski račun.

Za odabir lozinke za pristup računalu preporučeno je koristiti najmanje 8 znakova, kombinaciju velikih i malih slova te brojeva i znakova. Preporučeno je ne upotrebljavati istu lozinku za više različitih računa.

Članak 14.

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

Od učenika se očekuje da prihvate filtriranje određenih sadržaja kao sigurnosnu mjeru te je zabranjeno svako zaobilaženje tih mjera jer su one postavljene radi njihove sigurnosti i sigurnosti drugih učenika. Također, zaobilaženje sigurnosnih postavki može ugroziti održavanje nastave. Učenici su upoznati s informacijama o filtriranju nepoćudnih sadržaja što im se posebno naglašava te se o istome educiraju i upućuju na nastavi Informatike, Računalstva i Računarstva. U Školi postoji nadzor mrežnog prometa kroz Meraki Cloud System od strane e-Škole tehničara.

V. Sigurnost korisnika

Članak 15.

U školama je potrebna stalna edukacija učenika, nastavnika i cijelog školskog kolektiva kako bi se držao korak s trendovima u korištenju IKT-a, kao i s nadolazećim prijetnjama računalnoj sigurnosti.

Članak 16.

Kod prijave na računala i u aplikacijama koje zahtijevaju autentifikaciju, svi korisnici dužni su posebno voditi računa da ne otkriju svoje pristupne podatke.

Isto tako kada nastavnici 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 obvezno se moraju odjaviti iz sustava u koji su se prijavili.

Članak 17.

Učenici, nastavnici 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. Ostali računi ograničeni su pa takva vrsta interakcije nije dopuštena.

Članak 18.

Svi učenici, nastavnici i ostali djelatnici posjeduju elektronički identitet u sustavu AAI@Edu.hr. Na početku svake godine izvodi se ponovna evidencija korisničkih računa – 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, administratorica e-Dnevnika ispisuje korisnički račun s novom ili po zahtjevu sa starom lozinkom. U slučaju da učenik seli iz naše u drugu školu, njegov korisnički identitet odjavljuje se s datumom odlaska. U slučaju da učenik iz druge škole dolazi u našu njegov elektronički identitet se prenosi u našu školu. Isto vrijedi i za djelatnike škole.

Učenicima prestaju prava nad elektroničkim identitetom kada završe sa svojim školovanjem, a nastavnicima i ostalim djelatnicima prestaju prava kada završe sa svojim radnim vijekom, tj. odlaskom u mirovinu ili prestankom rada u školskom sustavu.

VI. Prihvatljivo i odgovorno korištenje IKT-a

Ponašanje na internetu

Članak 19.

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

Općeprihvaćeni skup pravila ponašanja na internetu – *Netiquette* dostupan je svim učenicima u učionicama Informatike. Nastavnici predmeta Informatika, Računalstvo i Računarstvo dužni su učenike poučiti o navedenim pravilima.

U slučaju učeničkog nepridržavanja *Netiquette* pravila koje može za posljedicu imati vrijeđanje druge osobe ili objavljivanje neprimjerenih sadržaja, Škola je dužna pridržavati se Pravilnika o izricanju pedagoških mjera.

Učenici također na nastavi Informatike, Računalstva i Računarstva trebaju biti upoznati s činjenicom da ni u kojem slučaju ne otkrivaju svoje osobne podatke, uključujući svoju adresu, ime škole, telefonske brojeve i slično.

Članak 20.

Pravila ponašanja koja proizlaze iz *Netiquette*-a možemo promatrati kroz tri oblika:

1. **ELEKTRONIČKA POŠTA:**

   - *Nesigurnost* – ako se ne upotrebljavaju metode zaštite, elektronička pošta na internetu nije sigurna. U nju se nikada ne smiju stavljati podatci koje ne bi napisali na razglednicu.
   - *Poštivanje autorskih prava* – potrebno je poštivati prava vlasnika nad materijalima koji se upotrebljavaju jer sve zemlje imaju zakone o vlasničkim pravima.
   - *Prosljeđivanje poruka* – ako se prosljeđuje poruka koju je korisnik primio, ne smije joj mijenjati sadržaj, već treba zatražiti dopuštenje autora ako je prosljeđuje grupi ljudi. Ukoliko iz izvorne poruke, preuzima samo njezine dijelove i šalje drugima, onda treba navesti autora izvornog teksta.
   - *Lanci sreće* – ne smiju se nikada slati elektroničkom poštom jer su na internetu zabranjeni. Sudjelovanjem korisniku može biti uskraćen pristup mreži.
   - *Adresa pošiljatelja* – mnogi programi za e-mail izbrišu podatke iz zaglavlja koji sadrže adresu za odgovor. Da bi primatelji poruke bili sigurni da znaju tko je pošiljatelj, potrebno je uključiti liniju ili dvije na kraju poruke s podatcima za kontakt. Moguće je napraviti datoteku s kontaktnim podatcima i uključivati ga na kraju poruke. Neki programi to rade automatski. U internetskom žargonu to je poznato kao signature datoteka – ona će nadomjestiti posjetnicu, a moguće ih je imati nekoliko za različite prigode. Ona treba bit kratka, ne više od četiri linije.
   - *Primatelj pošte* – potrebno je obratiti pozornost kome se šalje e-mail. Postoje adrese koje predstavljaju grupu ljudi, a izgledaju kao da se radi o jednoj osobi.
   - *Sadržaj i smisao pošte (tekst poruke)* – primatelji pošte mogu biti ljudi različitog jezika, kulture, stavova i smisla za humor, zato je potrebno biti oprezan s

pisanjem datuma, mjernih jedinica, idioma, a posebno upotrebom humora ili sarkazma u tekstu.

- *Poštivanje pravopisa* – poštivanje pravopisnih pravila vrijedi i za elektroničku poštu. U tekstu poruke potrebno je poštivati pravopisna i gramatička pravila pojedinoga jezika. Nije preporučljivo koristiti se samo velikim slovima jer odaju dojam vikanja. Poželjno je upotrebljavati emotikone da bi se naznačili osjećaji, ali ih treba upotrebljavati s mjerom.
- *Troškovi elektroničke pošte* – troškove elektroničke pošte snose i pošiljatelj i primatelj (ili njihove organizacije). Primatelj može imati troškove kao što su širina internetske veze (bandwith), diskovni prostor ili korištenje procesora. To je ekonomski razlog zašto je oglašavanje elektroničkom pošteom katkad 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. Ako se šalje prevelika datoteke, postoji mogućnost da iste neće biti poslane zbog prevelike količine podataka.

Članak 21.

2. POPIS E-ADRESA (mailing liste, news grupe)

- Potrebno je čitati poruke u *mailing* listi i *news* grupi nekoliko mjeseci prije nego što na njih nešto pošaljete. To će pomoći razumjeti pravila ponašanja grupe.
- Za neodgovorno ponašanje korisnika, odgovornost i krivnju ne preuzima sustav 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).
- Potrebno je znati da elektronička pošta i *news* grupe troše resurse sustava, stoga treba paziti na sva pravila koja pojedina organizacija ili institucija ima o korištenju tih resursa.
- Poruke i članci trebaju biti kratki i u vezi s onim o čemu se raspravlja, ne smije se skretati s teme, potrebno je suvislo se izražavati te nije preporučljivo ispravljati tuđe pogreške.
- U elektroničkoj komunikaciji lažno predstavljanje nije dopušteno.
- Oglašavanje je dopušteno na nekim listama i grupama, a osuđivano na drugima. Zato je važno upoznati sudionike liste ili grupe prije slanja poruke. Neželjene reklamne poruke, koje se ne tiču teme rasprave, sigurno će uzrokovati nezadovoljstvo ostalih sudionika ili je moguće izgubiti pravo pristupa internetu.
- Ako korisnik sudjeluje u raspravi, treba pročitati sve članke u nizu (*thread*) prije nego što pošalje odgovor. Sadržaj poruke treba proširivati onu na koju se nadovezuje. Nije preporučljivo slati poruke: „Ja također“.
- Poruku koja se tiče samo jedne osobe treba slati elektroničkom poštom. *News*-e treba upotrebljavati samo ako korisnik ima informacije korisne sudionicima u raspravi. Ako korisnik misli da je članak zanimljiv većem broju grupa, potrebno je upotrebljavati *crosspostate* i ne ga slati svakoj grupi posebno.
- Prije postavljanja pitanja na *newsi*ma poželjno je upotrebljavati priručnike, knjige, datoteke za pomoć i sl. jer odgovori na pitanja možda već postoje na drugim mjestima.

- U *news* člancima nije dopušteno lažno se predstavljati. Od toga se moguće zaštititi korištenjem programa koji generira „otisak prsta“ (PGP).

Članak 22.

3. FORUMI

- Ako postoje pravila foruma, potrebno ih je obvezno pročitati i pridržavati ih se.
- Ako postoji popis često postavljanih pitanja (FAQ – *Frequently Asked Questions*), korisnik ga obvezno treba pročitati jer se tamo već možda nalazi tražena informacija.
- Korisnik treba dobro pregledati forum i biti siguran da započinje raspravu u pravom dijelu foruma.
- Prije nego li korisnik započne temu, trebao bi pretražiti forum i potražiti sličnu temu. Možda već postoji rasprava poput one koju namjerava započeti.
- Naslov teme mora biti kratak i jasan. Odnosno, iz naslova mora biti jasno o kojoj je temi riječ.
- O sadržaju poruke potrebno je razmisliti i pažljivo sročiti poruku objavljivanja. Poruka treba biti jasna i smislena.
- Poželjno je pisati u prijateljskom tonu i izbjegavati nesporazume koliko god je to moguće.
- Kada korisnik nastavlja raspravu, potrebno je pročitati svoje prijašnje poruke kako bi bio siguran da neće dodati informaciju koja već postoji.
- Ako korisnik u vrlo staru temu dodaje novu poruku, mora biti siguran da je ona vrijedna toga.
- Nepoželjno je upotrebljavati isključivo velika slova jer ona odaju dojam vikanja.
- Kod odgovora (reply), citirajte poruku na koju odgovarate.
- Ako je poruka na koju korisnik odgovara dugačka, citirati treba samo bitne dijelove.
- Privatni razgovori na javnom dijelu foruma nisu poželjni. Za njih treba upotrebljavati privatne poruke, ako postoje, ili e-mail.
- Potpisi korisnika trebaju biti što kraći i neupadljivi.
- Nije poželjno stavljati slike u potpise.

Članak 23.

Pravila sigurnog ponašanja

Osim pravila lijepog ponašanja, učenici su na isti način upoznati i s Pravilima sigurnog ponašanja. Učenike se poučava kroz nastavu Informatike, Računalstva, Računarstva i satova razrednika da ne otkrivaju osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično na servisima poput Facebooka, Twitera, chat sobe itd., a pritom se trebaju pridržavati sljedećih pravila:

- osobne informacije na internetu se nikad ne smiju odavati
- zaporka je tajna i nikad se ne smije nikome reći
- ne odgovarati 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

- potrebno je provjeriti je li Facebook profil skriven za osobe koji nam nisu „prijatelji“. Treba biti kritičan prema ljudima koji se prihvaćaju za „prijatelje“
- potrebno je biti oprezan s izborom fotografija koje se objavljuju na Facebooku
- potrebno je provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (upisati svoje ime i prezime u Google).

VII. Autorsko pravo

Članak 24.

Autorska prava na online dokumentima najčešće se definiraju s tzv. *Creative Commons* (CC) licencama (više na: https://creativecommons.org/licences/?lang=hr.). *Creative Commons* licence su skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Svaka od licenci pomaže autorima da zadrže svoja autorska prava, a drugima dopuštaju umnožanje, distribuciju i na neke druge načine korištenje njihova djela, barem u nekomercijalne svrhe. Svaka CC licenca osigurava davateljima licence da ih se prizna i označi kao autore djela.

Članak 25.

Sve korisnike školske IKT infrastrukture potiče se da potpisuju materijale koje su sami izradili koristeći neku licencu, ali isto tako da poštuju i tuđe radove.

Korisnici nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti nedozvoljeno preuzimati tuđe radove s interneta. Korištenje tuđih materijala s interneta mora biti citirano, obvezno navodeći autora korištenih materijala te izvor informacija (poveznica i datum preuzimanja).

Članak 26.

Računalni programi također su zaštićeni zakonom kao 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 mrežnog 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.

VIII. Dijeljenje datoteka

Članak 27.

Prednost digitalnog sadržaja jest da se ne uništava ili mu se ne umanjuje kvaliteta brojem umnažanja. No, upravo zbog toga je potrebno biti vrlo oprezan s upotrebom digitalnih materijala, a još više s njihovim dijeljenjem.

Dijeljenje datoteka, samo po sebi, nije nezakonito, no danas postoje razni primjeri nezakonitog dijeljenja datoteke: umnažanje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak videosadržaja. Mnogi *online* servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, videosadržaja ili e-knjiga na nezakonit način. Primjer su klijenti (npr. *Torrent*) koji omogućuju dijeljenje sadržaja između računala pa se tako dijele najčešće nezakonito nabavljeni videosadržaji te glazbeni sadržaji, ključevi za korištenje različitih aplikacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, a gdje je izričito zabranjeno daljnje distribuiranje i umnožavanje bez dozvole autora ili bez plaćanja naknade.

Postoje i različiti oblici mrežnog servisa koji omogućuju registraciju korisnika za vrlo nisku mjesečnu pretplatu te nude preuzimanje gotovo neograničene količine digitalnog sadržaja koji je zaštićen autorskim pravom, no to je također nezakonito.

Članak 28.

Prema Pravilniku, svim korisnicima školske infrastrukture je izričito zabranjen bilo kakav oblik nezakonitog dijeljenja datoteka.

Obveze ustanove su:

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

IX. Internetsko nasilje

Članak 29.

Internetsko nasilje općenito se može definirati kao namjerno i opetovano nanošenje štete upotrebom 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 nasilja:

- Nastavljanja slanja e-pošte usprkos tome šte netko više ne želi komunicirati s pošiljateljem
- 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 uznemirujućih i/ili prijetećih poruka žrtvi koristeći različite internetske servise (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
- Krađa ili promjena lozinke za e-mail ili nadimka na chatu

Članak 30.

Nasilje u školama postaje sve veći problem tijekom nekoliko posljednjih godina jer se sve više djece koristi internetom i mobilnim telefonima za komuniciranje pa internetsko nasilje „cyberbullying“ postaje veliki problem.

Međuvršnjačko nasilje putem interneta uključuje poticanje grupne mržnje, napade na privatnost, uznemiravanje, uhođenje, vrijeđanje, nesavjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih komentara. Može uključivati slanje okrutnih, zlobnih, katkad i prijetećih poruka, kao i kreiranje internetskih stranica koje sadrže priče, crteže, slike i šale na račun vršnjaka.

Cyberbullying se najčešće izvodi oblicima komunikacije u kojima identitet počinitelja može biti skriven. Nedostatak socijalnih i kontekstualnih naznaka, kao što su govor tijela i ton glasa, može imati mnoštvo učinaka: nema opipljive, afektivne povratne informacije o tome je li ponašanje preko interneta prouzročilo štetu drugome.

Anonimnost počiniteljima nasilja preko interneta daje osjećaj da nekažnjeno mogu kršiti socijalne norme i ograničenja što rezultira već navedenim ponašanjem.

Članak 31.

Edukacija o neprihvatljivom ponašanju provodi se kroz Informatiku, Računalstvo, Računarstvo i Sate razrednika te su pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva u prostorijama Škole.

Škola se obvezuje da će provoditi preventivne mjere suzbijanja nasilja na slijedeći način:

- podučiti učenike i nastavnike o mogućim oblicima internetskog nasilja
- podučiti učenike i nastavnike kako prepoznati internetsko nasilje

- jasno istaknuti prihvatljiva pravila ponašanja te učenike i nastavnike podučiti o njima kroz predmete na kojima se upotrebljava IKT.
- izraditi strategiju odgovora na internetsko nasilje i to na blaži i teži oblik (vidi čl. 31.).
- razvijati nultu stopu tolerancije na internetsko nasilje.
- 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.

Članak 32.

Svi su oblici nasilničkog ponašanja nedopušteni, a svi oni za koje se utvrdi da provode takve aktivnosti, bit će sankcionirani u skladu s Pravilnikom o kriterijima za izricanje pedagoških mjera čl. 3, Pravilnikom o načinu postupanja odgojno – obrazovnih radnika školskih ustanova u poduzimanju mjera zaštite prava učenika, te prijave svakog kršenja tih prava nadležnim tijelima čl. 18., 19., 20. i Kućnim redom Škole.

X. Uporaba mobilnih telefona

Članak 33.

Kućnim redom Škole čl. 35 zabranjena je upotreba mobitela za vrijeme nastave. U slučaju prekršaja, nastavnik može privremeno oduzeti mobitel učeniku i zadržati ga do kraja nastavnog sata na svom stolu, nakon čega će ga vratiti učeniku. O tome će obavijestiti razrednika i unijeti napomenu u e-dnevnik.

Učenici se mogu koristiti mobitelom na nastavnim satima samo uz dopuštenje predmetnih nastavnika i u svrhu odgojno-obrazovnog procesa kao nastavno pomagalo.

Učenici se mogu koristiti mobitelom tijekom odmora te prije i poslije nastave.

Članak 34.

Jedan od popularnih oblika nasilja među vršnjacima koje donosi suvremeno doba tehnologije je i nasilje putem mobitela. Ono uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti – tekstualna poruka, videoporuka, fotografija, poziv – odnosno bilo kakva višestruko slana poruka kojoj je cilj uvrijediti, zaprijetiti ili/i nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Škola će kroz predmete Informatika, Računalstvo, Računarstvo i Sat razrednika informirati učenike, a kroz roditeljske sastanke roditelje o posljedicama zlouporabe mobilnih telefona i o pravilima sigurnog korištenja mobitela:

- vođenje računa o tome kome se daje broj mobitela.
- opreznost pri korištenju nekih od *chat* usluga preko mobitela
- neodgovaranje na poruku primljenu s nepoznatog broja
- neodgovaranje na poznate brojeve ako se zbog sadržaja poruke osjećamo loše ili neugodno

- opreznost i razmatranje pri slanju poruku čiji sadržaj može uvrijediti ili na bilo koji način naštetiti toj osobi
- zabrana slanja fotografije ili videozapise drugih ljudi bez njihova dopuštenja, kao ni slanje sadržaje koji mogu uvrijediti druge ljude
- davanje podrške učeniku koji dobije neprimjerenu poruku, poziv ili je izložen nasilju, i poticanje na razgovar s odraslom osobom u koju ima povjerenja (nastavnik, pedagog), kako se problem ne bi pogoršao.
- svaki ozbiljniji oblik nasilja, osobito zastrašujuće prijetnje treba odmah prijaviti policiji te je dobro u takvim slučajevima sačuvati poruke u mobitelu ili negdje drugdje zapisati podatke o datumu, vremenu i sadržaju poruke ili poziva.

Članak 35.

Mobilni telefoni sve više imaju potpuni pristup internetu te djeca i mladi upotrebljavaju 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 sl.).

Članak 36.

Ovaj Pravilnik stupa na snagu danom donošenja.

KLASA: 003-05/18-01/02
URBROJ: 2127-024-08-18-01
Grubišno Polje, 10. srpnja 2018.

Predsjednica Školskog odbora
Kristina Vrbicki, mag. educ., v.r.