**OSNOVNA ŠKOLA IVANA GORANA KOVAČIĆA**

**MESIĆEVA 35**

**10000 ZAGREB**

**PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO- KOMUNIKACIJSKE TEHNOLOGIJE**

Zagreb, 2021.

Na temelju odredbe članka . Statuta Osnovne škole Ivana Gorana Kovačića Školski odbor Osnovne škole Ivana Gorana Kovačića, a na prijedlog ravnatelja na sjednici održanoj 8.ožujka 2021. godine donosi

**PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE (IKT) U ŠKOLI**

**I. 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. Ljudski i informacijski resursi smatraju se najvažnijim vrijednostima Osnovne škole Ivana Gorana Kovačića (u daljnjem tekstu: Škola). Zbog toga je potrebno veliku pozornost posvetiti obliku sigurnog i odgovornog korištenja IKT-a, što je moguće postići definiranjem sigurnosne politike Škole.

Članak 2.

Ovaj Pravilnik vrijedi za sve korisnike IKT Škole.

U Školi je postavljena infrastruktura Hrvatske akademske i istraživačke mreže - CARNet (u daljnjem tekstu: CARNet).

Učenici i zaposlenici moraju se pridržavati uputa za nesmetano i sigurno korištenje IKT-a koje im može dati administrator (tehničar) i administrator e-Dnevnika Škole.

Članak 3.

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije dio je sigurnosne politike Škole. Oblikovan je uzimajući u obzir preporuke Izvršne agencije za obrazovanje, audiovizualnu djelatnost i kulturu (u daljnjem tekstu: EACEA/Eurydice ), 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,

• jasnog definiranja 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 mlade,

• poticanja aktivnog sudjelovanja djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici,

• propisivanja sankcija u slučaju kršenja odredbi Pravilnika.

Cilj je sigurnosne politike Škole propisati odredbe koje imaju za cilj upravljanje svim primjenjivim aspektima sigurnosti informacijskih sustava. Njime se propisuju obveze i prava korisnika informacijskih sustava, raspodjela odgovornosti, plan održavanja, dokumentiranje sustava itd. Nadalje, sigurnosna politika mora obuhvatiti i područje upravljanja rizicima, incidentima te postupcima kako se oporaviti od incidenta.

Većina mjera zaštite implementirana je od strane davatelja internetskih usluga - CARNet. Njihovi serveri blokiraju sadržaje i stanice sumnjivog karaktera.

**OSNOVNE SIGURNOSNE ODREDBE**

Članak 5.

Materijalni i nematerijalni resursi

• korisnici IKT infrastrukture su učenici, nastavnici, ostali zaposlenici i povremeni korisnici,

• kompletna računalna mreža izgrađena u projektu e-Škole i dio računalne opreme dobivene kroz isti projekt te ranije izgrađena školska računalna mreža te školska oprema nabavljana sredstvima Škole i donacijama ( računala, pametne ploče, LCD projektori, pisači, tableti, sustav za nadzor, telefonska centrala, itd.) smatraju se IKT infrastrukturom.

• virtualnim školskim prostorom smatra se školsko mrežno mjesto http://os-igkovacic-zg.skole.hr/ i sva službena školska mjesta na društvenim mrežama te svako mrežno mjesto na kojem se učenici i zaposlenici Škole javljaju kao njeni službeni predstavnici.

Članak 6.

Ciljevi mjera informacijske sigurnosti koje se primjenjuju na računalnu mrežu su:

• omogućavanje elektroničke komunikacije,

• neometano korištenje informacija koje su putem računalne mreže dostupni,

• zaštita školske računalne mreže,

• zaštita osjetljivih podataka Škole.

Članak 7.

Načelo povjerljivosti informacija podrazumijeva da informacije moraju biti dostupne samo onome kome su namijenjene. U skladu s time, Škola razlikuje javne i povjerljive informacije:

• Skupinu javnih informacija čine one informacije koje opisuju djelatnosti Škole, a njihova javna dostupnost je u interesu Škole. Tu spadaju kontakt podatci Škole, promidžbeni materijal i ostale informacije s mrežne stranice, informacije koje je Škola u skladu sa zakonima dužna objavljivati.

• Povjerljive informacije su one koje se odnose na osobne podatke pojedinca (npr. kontakt podatci, fotografija osobe), podatci 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 odobrenje ravnatelja ili osobe koju on za to opunomoći.

Članak 8.

Škola koristi brojne službene aplikacije u svrhu prikupljanja, obrade i slanja podataka: e-Dnevnik, e-Matica, HUSO admin, Centralni obračun plaća COP, e-HZMO, MDM, Centralni registar Grada Zagreba, program za rad u knjižnici, programski paket za računovodstveno poslovanje MIPSED 7, Registar zaposlenih u javnom sektoru, aplikaciju za interaktivno upravljanje učionicom LanSchool, Office 2019, OS Windows 8/10.

Zaposlenici zaduženi za unos podataka obvezni su čuvati povjerljive informacije te iste ne smiju prosljeđivati neovlaštenim osobama. Zaposlenici Škole zaduženi za unos i čuvanje navedenih podataka trebaju svoja računala zaštititi lozinkom koju ne smiju davati neovlaštenim osobama.

Tuđe osobne podatke zabranjeno je koristiti bez dopuštenja - privole osobe.

Poslovnu dokumentaciju važnu za poslovanje Škole potrebno je čuvati na zakonom propisan način.

Članak 9.

Sigurnosne mjere zaštite podataka u školi su, s obzirom na dostupnost financija, na prosječno zadovoljavajućoj razini. Sva računala koja se koriste za uredsko poslovanje (tajništvo, računovodstvo, ravnateljstvo, stručna služba, zbornica, knjižnica, Škola u bolnici, zaštićena su antivirusnim programom Kaspersky. Učiteljska prijenosna računala i računala u informatičkim učionicama zaštićena su Windows Defender antivirusnim programom.

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 su upoznati s informacijama o sustavu, odnosno da je sustav podešen tako da filtrira nepoćudan sadržaj te im se to posebno naglašava i o istome se educiraju.

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.

Članak 10.

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 www.cert.hr (Computer Security Incident Response Team), organizacijskom entitetu koji reagira na računalno-sigurnosne incidente te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava.

**III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE**

Članak 11.

Računalna mreža je skup povezanih računala koja omogućuju brzu razmjenu podataka neovisno o njihovoj udaljenosti. Računalnu mrežu Škole čine sva stolna i prijenosna računala i tableti u učionicama, informatičkim učionicama, zbornici, pratećim službama, knjižnici, te u Školi u bolnici.

Računala u školi su povezana bežično i žičano. Računalna mreža se sastoji od novog dijela koje je izgrađen u sklopu projekta e-Škole projekta te starog dijela mreže. Škola koristi usluge vanjskog trgovačkog društva koje je zaduženo i plaćeno za održavanje računala i mrežne infrastrukture.

U sklopu projekta e-Škole imenovan je stručnjak za tehničku podršku koji je zadužen za održavanje navedene mrežne infrastrukture i održavanja prijenosnih računala nastavnika dobivenih u sklopu projekta.

Sva oprema dobivena kroz projekt e-Škole u vlasništvu je CARNET-a te po završetku projekta (2022. godine) vlasništvo prelazi na Školu koja je zadužena za održavanje i pravilno korištenje opreme.

Članak 12.

Obzirom da je električni i elektronični otpad (EE otpad) klasificiran kao opasni otpad, on se mora skupljati i odvoziti odvojeno od ostalog otpada. Računalni otpad odvozi ovlaštena tvrtka za prikupljanje elektroničkog otpada.

Članak 13.

U bežičnim pristupnim točkama postavljena su tri naziva za pristup bežičnoj mreži (SSID): eduroam, eSkole, guest.

Većina računala u školi spojena su žičano na mrežu eduroam. To su računala u svakoj od učionica koje nastavnici koriste u radu, računala u informatičkim učionicama, zbornici, računovodstvu, tajništvu, knjižnici i pratećim službama.

Bežično su na mrežu spojeni tableti učenika, nastavnička prijenosna računala te učenički i nastavnički pametni telefoni.

Računala se bežično spajaju na mrežu putem pristupnih točaka koje se smještene u svakoj učionici, blagovaonici, knjižnici, zbornici i pratećim službama.

Članak 14.

Postavke na računalima koje koriste učenici podešene su na općenite te je na svim računalima postavljeno da kod prijave u operativni sustav nema zaporke. Svi operativni sustavi u Školi licencirani su i besplatno preuzeti od Ministarstva znanosti i obrazovanja.

**IV.REGULIRANJE PRISTUPA IKT OPREMI**

Članak 15.

Računalnoj mreži mogu pristupiti učenici, nastavnici, ostali djelatnici škole te vanjski partneri i posjetitelji. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske žičane mreže.

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

Članak 16.

Učenici smiju koristiti računala samo uz dopuštenje zaposlenika. Pristup aplikacijama i internetskim sadržajima određuje isključivo zaposlenik.

Učenici ne smiju instalirati dodatne računalne programe na računala (igrice ili nekakav drugi program) bez odobrenja administratora.

Članak 17.

Zaposlenici i učenici koji koriste informatičku opremu moraju se pridržavati navedenih odredbi:

• učionice moraju ostaviti uvijek na kraju onako kako su je zatekli,

• računala se obavezno moraju ugasiti nakon uporabe,

• u slučaju kvara računala obavijestiti administratora ili ravnatelja,

• radna mjesta moraju ostati čista i uredna (namješteni tipkovnica, miš, monitor i stolica na svome mjestu).

Članak 18.

Ulaz u operativne sustave na računalima u tajništvu, računovodstvu, uredu ravnatelja, uredu pedagoga i psihologa, knjižnici te računala u zbornicama i računala učitelja zaštićen je korisničkom zaporkom.

**V. SIGURNOST KORISNIKA**

Članak 19.

Svi učenici i nastavnici imaju elektronički identitet u sustavu [AAI@Edu.hr](mailto:AAI@Edu.hr). Učenici dobivaju elektronički identitet koji im se daje na čuvanje i korištenje. U slučaju da izgube svoj korisnički račun, učenik ili roditelj obraćaju se administratoru imenika Škole koji im daje novu lozinku.

Ukoliko učenik napušta Školu njegov elektronički identitet se briše. Učenicima prestaju prava nad elektroničkim identitetom kada završe sa svojim školovanjem.

Učenici moraju posebno voditi računa o svojem digitalnom identitetu koji su dobili iz sustava AAI@edu i Office-365 korisničkih podataka. Svoje podatke moraju čuvati.

Korisnici moraju voditi računa da, prilikom prijave na ona računala i programe koji zahtijevaju prijavu, ne otkriju svoje podatke za prijavu.

Članak 20.

Zaposlenici Škole posjeduju AAI@EduHr korisnički račun. Sustav AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj.

Preporuka zaposlenicima je da koriste školski e-mail ime.prezime@skole.hr u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja. Zaposlenici su dužni koristiti isti e-mail i za sve edukativne svrhe (e-Matica, e-Dnevnik i sl.).

Zaposlenicima prestaju prava kada završe sa svojim radnim vijekom, tj. odlaskom u mirovinu ili prestankom rada u školskom sustavu.

Zaposlenici moraju posebno voditi računa o svojem digitalnom identitetu koji su dobili iz sustava AAI@edu i Office-365 korisničkih podataka. Svoje podatke moraju čuvati.

Korisnici moraju voditi računa da, prilikom prijave na ona računala i programe koji zahtijevaju prijavu, ne otkriju svoje podatke za prijavu. Isto tako, zaposlenici se prilikom odlaska iz učionice (kada ostavljaju računalo uključeno) obavezno moraju odjaviti iz svih sustava u koje su se prijavili.

Članak 21.

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.

Za svakog korisnika koji se susreće s Internetom nužno je upoznavanje s osnovnim pravilima ponašanja u takvoj komunikaciji i takvom 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.

Škola će ovaj skup pravila učiniti dostupnim svojim učenicima, o tome ih podučiti, te primijeniti vlastitu politiku u skladu s tim pravilima.

Članak 22.

Pravila sigurnog ponašanja na Internetu su:

* Osobne informacije na Internetu nikad se 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 prikriva i da se odmah obavijeste odrasli.
* Potrebno je biti oprezan s izborom fotografija koje se objavljuju na društvenim mrežama.

Prilikom korištenja i objavljivanja sadržaja na Internetu, korisnici se moraju pridržavati sljedećih uputa:

• svi korisnici moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na Internetu,

• odgovorni korisnici svojim potpisom stoje iza sadržaja koji objave,

• svaki korisnik mora dobro balansirati između privatnih i školskih informacija koje dijele s drugima,

• korisnici moraju biti pažljivi koje podatke objavljuju na Internetu jer time utječu na svoju sigurnost i zaštitu svoje privatnosti,

• poštivati autorska prava, tj. tuđe radove ne smiju prikazivati kao svoje, niti nedozvoljeno preuzimati tuđe radove s Interneta,

• uravnotežiti vrijeme korištenja Interneta, tj. umjerenosti u korištenju.

Prilikom korištenja elektroničke pošte treba imati na umu:

* Elektronička pošta na Internetu nije sigurna, nemojte nikada staviti u e-mail ono što ne biste stavili na dopisnicu.
* Ukoliko prosljeđujete poruku koju ste primili, ne mijenjajte sadržaj. Ako je to bila osobna poruka upućena vama i vi je preusmjeravate grupi, zatražite dopuštenje. Možete ju kratiti i citirati samo dijelove od značaja, ali naznačite njezinog autora.
* Primatelj je ljudsko biće, čija se kultura, jezik i smisao za humor mogu razlikovati od vaših.
* Ne šaljite velike količine podataka ljudima koji ih nisu zatražili.

Članak 23.

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. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Zaposlenici i učenici potiču se da potpisuju materijale koji su sami izradili koristeći neku licencu te da poštuju tuđe radove. Nipošto tuđe radove ne smiju 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 naravno i online 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.

Nastavna sredstva (vizualna, auditivna, audio-vizualna i tekstualna) autorska su djela učenika ili nastavnika te kao takva podliježu autorskim pravima tj. ne smiju se umnožavati, distribuirati ili na neki drugi način koristiti bez suglasnost autora.

Članak 24.

Prednost digitalnog sadržaja je da se ne uništava ili mu se ne umanjuje kvaliteta s brojem kopiranja. Ipak, 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, dakako, uputno zaštititi djelo nekom vrstom prikladne licence.

Primjer nelegalnog dijeljenja datoteke jest kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak video sadržaja. Mnogi online servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, videosadržaja ili pak 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 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.

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 nelegalno.

U Školi se izričito zabranjuje nelegalno kopiranje ili preuzimanje autorski zaštićenog materijala.

Članak 25.

Računalna mreža postavljena je tako da u potpunosti onemogućava P2P (peer to peer) protokole i filtrira mrežne stranice koje sadrže P2P datoteke. U potpunosti je onemogućeno korištenje popularno zvanih Torrenata.

Obaveze ustanove su:

1. Učenike i zaposlenike podučiti o autorskom pravu i intelektualnom vlasništvu.

2. Učenike i zaposlenike 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 zaposlenike podučiti o načinima nelegalnog 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.

4. Učenike i zaposlenike informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Članak 26.

Elektroničko nasilje definira se kao ,,svaka zlonamjerna i ponavljana uporaba informacijskih i

komunikacijskih tehnologija kako bi se nekome nanijela šteta“ (Belsey, 2012; prema Bilić, Buljan

Flander i Hrpka, 2012, str. 301). Ono može biti počinjeno od strane pojedinca ili skupine te isto tako

može biti usmjereno pojedincu ili skupini. Nasilje preko Interneta, 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.

Elektroničko nasilje uključuje različite oblike ponašanja, a među najčešće navedenima u literaturi ističu se (Willard, 2005, 2007; Li, 2006; Beran i Li, 2007; Bilić, 2013; Bilić, 2016; Poliklinika za zaštitu djece i mladih, 2019):

• VRIJEĐANJE PORUKAMA (engl. flaming) – namjerno slanje neprimjerenih, uvredljivih i agresivnih poruka, s ciljem poticanja mrežnih sukoba i nasilja

• ONLINE UZNEMIRAVANJE (engl. harassment) – opetovano slanje poruka s uvredljivim sadržajem kako bi se uznemirilo i vrijeđalo drugu osobu

• Elektroničko UHOĐENJE I ZASTRAŠIVANJE (engl. cyberstalking) – ponavljajuće intenzivno

uznemiravanje koje uključuje prijetnje ili zastrašivanje pojedinca U literaturi se spominju brojni neprihvatljivi oblici ponašanja u virtualnom okruženju, kao što su, primjerice:

• zastrašivanje, slanje uznemirujućih i/ili prijetećih poruka

• omalovažavanje, vrijeđanje, izrugivanje, objavljivanje ponižavajućih komentara o nekome na društvenim mrežama, forumima, platformama

• objavljivanje i dijeljenje (intimnih) fotografija i/ili videozapisa putem društvenih mreža i aplikacija, snimljenih sa ili bez dozvole žrtve

• širenje glasina, istinitih i/ili lažnih informacija o drugoj osobi te ugrožavanje njezina ugleda (ali i članova obitelji i prijatelja)

• širenje povjerljivih informacija namijenjenih samo primatelju

• ignoriranje i/ili nepoštivanje nekog člana unutar postojeće grupe, blokiranje, izoliranje i socijalno isključivanje

• uhođenje putem društvenih mreža

• širenje virusa na drugi uređaj

• ELEKTRONIČKO KLEVETANJE (engl. denigration) i dezinformiranje (engl. misinformation) – slanje ili objavljivanje štetnih, neistinitih ili okrutnih izjava o nekoj osobi, što osobu može učiniti

neprivlačnom, ružnom ili odbojnom

• LAŽNO PRIKAZIVANJE (engl. masquerade) – pretvaranje osobe da je netko drugi te slanje ili

objavljivanje materijala koji narušavaju ugled te osobe

• ELEKTRONIČKO RAZOTKRIVANJE (engl. outing) i podvale (engl. trickery) – otkrivanje tajni,

(neugodnih) podataka, fotografija i privatnih informacija te njihovo slanje ili objavljivanje

• ISKLJUČIVANJE/OSTRACIZAM (engl. exclusion) – aktivnosti kojima se namjerno isključuje,

odbacuje ili briše osobu iz neke online grupe ili popisa prijatelja

• KRAĐA IDENTITETA (engl. impersonation) – krađa zaporki ili lažno predstavljanje, a zatim slanje

poruka i fotografija da se osoba dovede u opasnost ili našteti njezinu ugledu

• SNIMANJE/IZRADA VIDEO MATERIJALA NAPADA (engl. happyslapping) – napadanje, ismijavanje ili izvrgavanje ruglu vršnjaka od strane grupe te snimanje, a zatim slanje video snimki ili

objavljivanje istih na internetu

• SEKSTANJE (engl. sexting) – slanje ili primanje seksualno eksplicitnih ili seksualno sugestivnih

slika, poruka ili videa. Obično se odvija digitalnim putem, kroz SMS poruke, e-poruke ili instant

poruke. Seksting kao takav nije posebno rizičan, no može voditi prema neželjenom prosljeđivanju

poslanih materijala

• SEXTORTION (engl.) – oblik ucjene preko interneta koji uključuje neki oblik prijetnje, pri čemu

počinitelj najčešće prijeti da će objaviti i/ili proslijediti seksualno eksplicitne fotografije žrtve ako

se ona na neki način ne uključi u daljnje seksualne aktivnosti

• FRAPING (engl.) – nasilno upadanje „prijatelja“ na profile društvenih mreža i odašiljanje poruka

neprimjerenog sadržaja drugim osobama, kako bi izgledalo da to čine vlasnici profila; izvedenica

je riječi „Facebook“ i „raping“ (engl.)

• TROLLING (engl.) – namjerno širenje neprimjerenih komentara o slučajno odabranoj osobi s

ciljem izazivanja sukoba

• CATFISHING (engl.) – otvaranje lažnih profila pomoću kojih napadač navodi drugu osobu na

ljubavnu vezu putem interneta

• CYBERGROOMING (engl.) – proces u kojem odrasla osoba upoznaje dijete, zbližava se s njim i

stječe njegovo povjerenje („mamljenje“) s ciljem seksualnog zlostavljanja.

Članak 27.

Elektroničko vršnjačko nasilje postalo je sve veći problem tijekom nekoliko posljednjih godina.

Edukacija o neprihvatljivom ponašanju provodi se kroz predmete koji koriste tehnologiju ili Sat razrednika, te su pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva i u prostorijama Škole.

Škola će:

1. Podučiti učenike i zaposlenike o mogućim oblicima internetskog nasilja i o tome kako prepoznati internetsko nasilje.

2. Jasno istaknuti prihvatljiva pravila ponašanja te učenike i zaposlenike podučiti kroz predmete koji koriste tehnologiju te prilikom provođenja nastave na daljinu.

3. Izraditi strategiju odgovora na internetsko nasilje

4. Obilježavati Dane sigurnog korištenja Interneta i suzbijanja nasilja.

Škola će, prilikom rješavanja problema internetskog zlostavljanja, koristiti sve raspoložive oblike individualne i grupne pomoći i podrške. U težim slučajevima zlostavljanja ili ako se nasilje nastavi unatoč prethodno poduzetim mjerama savjetovanja, pomoći i podrške, Škola će djelovati sukladno Pravilniku o kriterijima za izricanje pedagoških mjera i Pravilnikom o načinu postupanja odgojno-obrazovnih radnika školskih ustanova u poduzimanju mjera zaštite prava učenika te prijaviti kršenja tih prava nadležnim tijelima.

Ukoliko Škola ima saznanja o bilo kojem obliku nasilja postupit će sukladno odredbama zakona te u suradnji s nadležnim institucijama i tijelima pokrenuti postupak radi zaštite prava učenika.

Stručna služba Škole provodit će savjetodavni rad s učenicima koji provode razne oblike uznemiravanja, a kroz strategiju će se provesti i preventivne mjere suzbijanja nasilja.

Članak 28.

Roditelji su partneri Škole u poučavanju učenika o sigurnoj upotrebi IKT-a te prevenciji bilo kakvog oblika zlouporabe te vrste tehnologije. Stoga je predviđeno povećano sudjelovanje roditelja u školskim aktivnostima u području IKT tehnologije. Škola će putem informativnih mailova i na roditeljskim sastancima informirati roditelje o sigurnoj uporabi informacijsko-komunikacijske tehnologije u školi i u nastavi na daljinu.

Članak 29.

Kućnim redom Škole propisano je da je zabranjeno korištenje mobitela u vrijeme nastave. Učenici mobilne uređaje na početku nastavnog sata ostavljaju u za to predviđenim kutijama.

Učenici mogu koristiti mobitel u slobodno vrijeme (mali odmor, veliki odmor) poštujući odredbe Pravilnika i Kućnog reda. U slučaju nedopuštenog korištenja, učitelj može mobilni uređaj privremeno oduzeti do kraja nastavnog sata. Kod ponovljenog korištenja učitelj će aparate predati razredniku. Razrednik u dogovoru s predmetnim učiteljem mobilni uređaj vraća učeniku ili poziva roditelja u školu.

Učenici mogu iznimno koristiti mobitele za vrijeme nastave kao nastavno pomagalo u dogovoru s predmetnim učiteljem. Svaka upotreba tehnologije u učionici mora imati unaprijed zadanu svrhu koja opravdava korištenje tehnologije.

Članak 30.

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.

Škola je dužna upoznati učenika s posljedicama zlouporabe mobitela te da je svaki oblik nasilja kažnjiv zakonom.

Ukoliko Škola ima saznanja o bilo kojem obliku nasilja postupit će sukladno odredbama zakona te u suradnji s nadležnim institucijama i tijelima pokrenuti postupak radi zaštite prava učenika.

Članak 31.

Nastava na daljinu

Škola omogućuje svim učenicima praćenje nastave na daljinu od kuće. Ukoliko učenik ne posjeduje uređaj ili nema mogućnost pristupa internetu za sudjelovanje u nastavi na daljinu potrebno se obratiti administratoru kako bi se osigurali dodatni uređaji.

Učenici su dužni pohađati nastavu na daljinu i pridržavati se pravila i uputa nastavnika kao na nastavi u školi.

Za provođenje nastave na daljinu preporuka Škole je uporaba alata MS Teams za koji nastavnici i učenici mogu dobiti podršku pri korištenju u školi. Svaki nastavnik može odlučiti koji program za nastavu na daljinu želi koristiti te treba biti upoznat s mogućnostima i uvjetima korištenja tih programa.

Prilikom sudjelovanja u nastavi na daljinu učenici su dužni:

* Koristiti svoje ime i prezime prilikom prijave
* Ukoliko se nastava održava u realnom vremenu putem videopoziva učenik treba imati uključenu kameru
* Zabranjeno je prosljeđivanje poveznica za videopozive nepoznatim osobama

Članak 32.

Postupanje prema odredbama ovog Pravilnika sastavni je dio radnih obveza radnika i učenika Škole.

Radnik koji postupi suprotno odredbama ovog Pravilnika, odgovoran je za težu povredu radne obveze.

Učenik koji postupi suprotno odredbama ovog Pravilnika, odgovoran je prema Statutu Škole.

Članak 33.

Svi izrazi koji se u ovom Pravilniku koriste u muškom rodu neutralni su te se odnose i na muške i na ženske osobe.

Ovaj Pravilnik objavit će se na mrežnim stranicama Škole, te stupa na snagu i primjenjuje se s danom objave.

KLASA:

Urbroj:

U Zagrebu, ožujka 2021.

Ravnatelj: Predsjednica Školskog odbora:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_