Na temelju članka 51. stavka 1. podstavka 2. Statuta Škole Školski odbor na 20. sjednici održanoj dana 12. travnja 2018.g.donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO KOMUNIKACIJSKE TEHNOLOGIJE Srednje škole Isidora Kršnjavoga Našice

I. Uvod

Članak 1.

S obzirom na sve veću sustavnu uporabu IKT tehnologija u školama, potrebno je voditi računa o prijetnjama informacijskom sadržaju i IKT infrastrukturi, a koje mogu rezultirati različitim oblicima štete u informacijskom sustavu (npr. gubitak informacija, nemogućnost pristupa resursima i informacijskom sadržaju, uništenje opreme i sl.). Iz navedenih je razloga potrebno posvetiti pozornost sigurnom i odgovornom korištenju IKT-a, što je moguće postići definiranjem sigurnosne politike Škole.

Članak 2.

Pravilnik vrijedi za sve korisnike IKT infrastrukture Škole u kojoj je 2017. godine postavljena infrastruktura CARNET mreže. Učenici se moraju pridržavati uputa nastavnika, a nastavnici i svi školski djelatnici uputa koje im može dati administrator IKT sustava (e-Škole tehničar). Zajednički cilj ovih uputa unapređenje je sigurnosti školske informatičke opreme i mreže.

U Srednjoj školi Isidora Kršnjavoga Našice administratorom IKT sustava (e-Škole tehničarem) imenovan je gospodin Zlatko Ibriks iz Zavoda za informatiku Osijek, čiji je osnivač Osječko-baranjska županija.

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

- unapređenja sigurnosti školske informatičke opreme i mreže
- jasnog određivanja načina prihvatljivog i dopuštenog korištenja IKT resursa Škole
- zaštite informacijskog sadržaja i opreme
- zaštite korisnika od različitih vrsta internetskog zlostavljanja
- promoviranja sustava i usluga koji su najprikladniji za djecu
- poticanja aktivnog sudjelovanja djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici

- pravilne raspodjele zadataka i odgovornosti nadležnih osoba
- propisivanja sankcija u slučaju kršenja odredbi Pravilnika.

II. Osnovne sigurnosne odredbe

Članak 3.

Kompletna računalna mreža (izgrađena, dobivena u sklopu pilot projekta e-Škole, stara računalna mreža i računalna oprema) smatra se IKT infrastrukturom Škole.

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

Materijalni resursi su:

- cjelokupna računalna oprema i mreža izgrađena i osigurana kroz pilot projekt e-Škole, stara računalna mreža i računalna oprema (pisači, projektori, pametne ploče i ostala oprema).

Nematerijali resursi su:

- aplikacije koje koristi Škola: e-Matica, e-Dnevnik, HUSO admin, CARNEtov CMS za škole, Office 2016, Windows 10, Office 365, računovodstveni program (COP, Riznica, ePorezna), knjižničarski program (Metel), sustav za upravljanje računalnom mrežom (Meraki).

Članak 4.

Školska oprema mora se čuvati i pažljivo koristiti.
Računalne učionice (interaktivna i pametna učionica, te postojeće računalne učionice) trebaju biti zaključane, učenici ne smiju ulaziti u navedene učionice bez prisustva nastavnika. Svaku štetu učenici i nastavnici dužni su prijaviti osobi odgovornoj za održavanje pojedine učionice. Svaku namjerno prouzročenu štetu učenik je dužan platiti.

Članak 5.

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 podaci Škole, promidžbeni materijali, internetske stranice Škole, informacije koje je Škola u skladu sa zakonom dužna objavljivati i sl.).

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

Osobni podaci djelatnika i učenika te osobni podatci Škole mogu se koristiti isključivo uz prethodno odobrenje ravnatelja ili osobe koju on za to posebno opunomoći.

Članak 6.

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

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

Većina je mjera zaštite implementirana kod davatelja internetskih usluga (ISP-a - CARNET). Njihovi serveri blokiraju sadržaje i stanice sumnjivog karaktera. U našem mrežnom sustavu blokiran je pristup P2P (peer to peer) mrežnom servisu za razmjenu podataka kao i web stranicama koje podržavaju P2P razmjenu podataka.

Članak 7.

Zaposlenici Škole posjeduju AAI@EduHr korisnički račun i dužni su koristiti službenu e - mail adresu (ime.prezime@skole.hr) za komunikaciju s nadležnim tijelima i institucijama iz sustava znanosti i obrazovanja.

Članak 8.

Nastavnicima i drugim djelatnicima Škole strogo je zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i digitalne identitete.

Članak 9.

Svi djelatnici Škole moraju potpisati izjavu o tajnosti podataka i moraju se pridržavati etičkih načela pri korištenju IKT-a.

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.

Ukoliko nastavnici ili drugi djelatnici Škole uoče bilo kakvo kršenje pravila opisanih ovim dokumentom, obvezni su navedeno prijaviti ravnatelju Škole.
Ukoliko učenici uoče bilo kakvo kršenje pravila opisanih ovim dokumentom, obvezni su navedeno prijaviti predmetnom nastavniku koji će isto prijaviti ravnatelju Škole.

Ozbiljniji incidenti prijavljuju se CARNET-ovom CERT-u, putem obrasca na mrežnoj stranici www.cert.hr.

III. Školska IKT oprema i održavanje

Članak 11.

Računala u Školi povezana su bežično i žičano. Računalna mreža sastoji se od novog dijela koje je izgrađen u sklopu pilot projekta e-Škole i starog dijela mreže. U sklopu e-Škole projekta osnivač Škole (Osječko – baranjska županija) imenovao je e-tehničara koji je zadužen i plaćen za održavanje navedene mrežne infrastrukture.

Članak 12.

Računalni otpad zbrinjava se odvojeno od ostalog otpada, a Škola će takav otpad predati ovlaštenom sakupljaču EE otpada.

Članak 13.

Računala se bežično spajaju na 32 bežične pristupne točaka. Pristupne točke smještene su u svakoj učionici, zbornici, holu Škole i sportskoj dvorani.

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

a) eduroam
b) eSkole
c) guest

Članak 14.

Određena računala u Školi spojena su žičanim načinom spajanja na mrežu. Uz minimalne troškove UTP kabel može se dovesti u bilo koju prostoriju ako se pojavi takva potreba. Računala koja su spojena na taj način spojena su na staru mrežnu infrastrukturu.

Računala koja su spojena žičano su sva računala u informatičkim učionicama i uredima (ured ravnatelja, tajništvo, računovodstvo, zbornica, ured pedagoginje, ured psihologinje).

Računalna mreža konfigurirana je tako da nema potrebe da se računala/korisnici autentificiraju kad se spajaju na žičanu računalnu mrežu.

Većina računala u Školi posjeduje operativni sustav Windows 10 s instaliranim Office 2016 alatima. Nekoliko starijih prijenosnih računala i računala u nekim informatičkim učionicama posjeduju Windows 7 operativni sustav s instaliranim Office 2010 alatima. U jednoj računalnoj učionici na 15 računala instaliran je Raspberry Pi. Postavke na računalima podešene su na općenite, kod prijave u operativni sustav nema zaporke. Također je uključena opcija da lozinka nikada ne ističe (Password never expires). Kod svih računala podešeno je ažuriranje operativnog sustava i popratnih office alata na automatski. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju putem interneta odlazi na ažuriranje navedenog. Operativni sustavi Windows 10 imaju u sebi obrambeni sustav (Windows Defender Security Center) te također i vatrozid koji posjeduju i stariji operativni sustavi do Winodws XP-a. Antivirusni programi ako se koriste, koriste se na starijim operativnim sustavima i to besplatne inačice antivirusnih programa (Malwarebytes Anti-Malware, AVG AntiVirus Free, Avast Free Antivirus). Od filtriranja sadržaja trenutno se filtriraju web stranice koje promoviraju i sadrže P2P (peer to peer) datoteke. Računalna mreža u potpunosti blokira promet P2P.

Članak 15.

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

Članak 16.

Svi računalni programi moraju se koristiti u skladu s propisima i pripadajućim licencama.

Učenici ne smiju instalirati nikakve računalne programe u informatičkoj učionici (igrice ili sl.). Na ostala računala u Školi nije moguće ništa instalirati bez odobrenja administratora. Ukoliko se pojavi potreba za instaliranje dodatnog računalnog programa, djelatnik- odnosno učenik koji ga želi instalirati- dužan je javiti se administratoru (u Školi je točno određeno tko je zadužen za održavanje pojedinog računala).

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.

IV. Reguliranje pristupa IKT opremi

Članak 17.

Računalnoj mreži mogu pristupiti učenici, nastavnici, ostali djelatnici Škole te vanjski partneri 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 školi su definirane tri bežične mreže (3 SSID-a):

- e-škole – služi za povezivanje tableta u STEM učionicama na bežičnu mrežu, odnosno za povezivanje uređaja koje koristi više različitih osoba
- eduroam – služi za povezivanje učenika, nastavnika i ostalog osoblja na bežičnu mrežu, odnosno za povezivanje uređaja kojeg u pravilu koristi samo jedna osoba
- guest – služi za povezivanje vanjskih posjetitelja i partnera na bežičnu mrežu.

Za pristup mreži **e-škole** koriste se sljedeći parametri:

- PSK (pre-shared key) za autentikaciju korisnika i pristup na bežičnu mrežu
- WPA2 enkripcija podataka na pristupnom sloju bežične mreže
- Captive portal za autentikaciju korisnika prilikom pristupa Internetu. Za autentikaciju se koristi AAI@EduHr baza korisnika.
- Captive portal se nalazi na poveznici https://prijava.e.skole.hr
- korisnici nakon pristupa u mrežu eSkole pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23.

Za pristup mreži **eduroam** koristi se sljedeći parametri:

- 802.1X enterprise RADIUS autentikacija uz WPA2 enkripciju podataka
- za pristup mreži eduroam koristi se protokol TTLS-PAP. Detaljnije upute se mogu naći na installer.eduroam.hr (installer se preporučuje za starije uređaje, odnosno na novim uređajima bi prijava na eduroam trebala raditi bez eduroam installera).
- za autentikaciju se koristi AAI@EduHr baza korisnika.
- korisnici nakon pristupa u mrežu eduroam pripadaju u VLAN 14 i imaju IP adresu iz mreže 192.168.38.0/23 osim ako se radi o djelatnicima koji tada pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23
- za navedenu se mrežu limitira ukupna propusnost na 50% (definirano za VLAN 14), osim ako se radi o djelatnicima koji su pozicionirani u VLAN 10 gdje nema ograničenja.

Za pristup mreži **guest** mreži koriste se sljedeći parametri:

- otvoren pristup mreži uz mogućnost Captive portal autentikacije za pristup na internet

- za autentikaciju se koristi baza korisnika iz Meraki dashboarda. Svakom gostu, kojem treba omogućiti pristup internetu, tehničar mora unijeti email adresu u Meraki dashboard kako bi mu omogućio pristup jer u startu nije kreiran niti jedan korisnik koji može pristupiti navedenoj mreži.
- korisnici nakon pristupa u mrežu guest pripadaju u VLAN 13 i imaju IP adresu iz mreže 192.168.36.0/23.
- za navedenu mrežu limitira se ukupna propusnost na 50% ukupne propusnosti linka prema internetu.

Svi korisnici koji pristupaju mreži autenticirani su na jedinstven način.

Učenici pristupaju mreži putem tableta u STEM učionicama (omogućen im je pristup na bežičnu mrežu eSkole; za pristup mreži i enkripciju prometa koristi se WPA2 PSK metoda; za pristup internetu i servisima svaki se učenik mora dodatno autenticirati putem tzv. Captive portala, korištenjem vlastitog AAI@edu računa; po završetku rada s tabletom svaki učenik dužan je odjaviti se s uređaja) ili putem vlastitih uređaja (omogućen im je pristup na bežičnu mrežu putem eduroam mreže; za autentikaciju na eduroam mrežu učenici koriste vlastiti AAI@edu račun).

Nastavnici i djelatnici Škole na bežičnu mrežu pristupaju putem vlastitih uređaja ili uređaja dobivenih u sklopu projekta. Budući da su uređaje dobivene u sklopu projekta (računala, tableti i sl.) osobno zadužili, nije planirano da koriste uređaje koje dijele s kolegama. Stoga nastavnici i djelatnici za pristup mreži koriste eduroam mrežu, te se autenticiraju vlastitim AAI@edu računom. Ako povremeno u STEM učionicama ipak koriste zajedničke tablete, moraju se, kao i učenici, preko Captive portala autenticirati na mrežu eŠkole. Na nastavničkim računalima (stolnim i/ili prijanosnim) u učionicama gdje se održava nastava, nastavnici za pristup mreži koriste mrežu eŠkole te se autenticiraju vlastitim AAI@edu računom.

Vanjski partneri i posjetitelji

Partnerima i posjetiteljima, koji imaju AAI@edu račun, omogućen je pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima može se, na njihov zahtjev, omogućiti pristup bežičnoj mreži. Bežična mreža guest otvorenog je tipa, a za autentikaciju se koristi tzv. captive portal. Kako bi im se omogućio pristup, „e-Škole“ tehničar u Meraki dashboardu mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Na postojećim računalima u računalnim učionicama, učenici se spajaju na postojeću CARNET – ovu mrežu koja je u Školi postojala prije ulaska u projekt e-Škole bez prethodne autentikacije.

Svi nastavnici su dobili računalo u sklopu projekta e-Škole. Nastavnici iz STEM područja su dobili hibridno računalo Lenovo ThinkPad Yoga 260, ravnatelj i stručne suradnice su dobili HP Elite prijenosno računalo, a ostali nastavnici tablet računalo HP 10 EE Z3735F.

U slučaju duže odsutnosti djelatnika, a u svrhu normalnog funkcioniranja nastavnog procesa, djelatnik je dužan vratiti opremu, o čemu odluku donosi ravnatelj.

Članak 18.

STEM učionice (učionice biologije i matematikea) opremljene su računalima koji učenici mogu koristiti samo uz odobrenje nastavnika. Nastavnici i ostalo osoblje također imaju pristup računalu u zbornici i smještenima u informatičkoj učionici. Učitelji ne moraju tražiti posebno odobrenje za korištenje informatičke učionice.

Učenici smiju koristiti računala samo uz dopuštenje nastavnika. Ukoliko su uspješno prošli sve etape nastavnog procesa i prethodno dobili odobrenje nastavnika za uključivanje računala, učenici smiju na kraju drugog sata (nastava informatike održava se u blok satu) i za vrijeme odmora koristiti računalo za svoje potrebe. U STEM učionicama učenici također smiju koristiti računalnu opremu samo uz odobrenje nastavnika. Pristup aplikacijama i internetskim sadržajima određuje isključivo nastavnik.

Vlastita računala i pametne telefone učenici smiju za vrijeme nastave koristiti 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 učenici mogu pristupiti, određuje isključivo nastavnik. Učenici smiju koristiti vlastita računala u privatne svrhe isključivo za vrijeme odmora te prije i poslije nastave.

Članak 19.

Osim računalima koja su dobili u sklopu pilot projekta e-Škole, nastavnici imaju pristup računalu u zbornici, kabinetima te, prema potrebi, računalima u informatičkoj učionici, a ostalo osoblje računalima u uredima Škole.

Članak 20.

Svi nastavnici koji koriste informatičku učionicu moraju se pridržavati sljedećih naputaka:

- učionica mora ostati na kraju nastavnog sata u istom urednom stanju u kakvom je i zatečena
- računala se obavezno moraju ugasiti nakon uporabe
- u slučaju da neko od računala ne radi, treba kontaktirati nastavnika informatike (voditelja informatičke učionice)
- radna mjesta moraju ostati uredna (namještena tipkovnica, miš, monitor, stolica na svojem mjestu)
- prozore obavezno zatvoriti na kraju radnog dana
- učionicu zaključati.

Nastavnik informatike (voditelj informatičke učionice) odgovoran je za informatičku učionicu.

Članak 21.

Trenutno je većina računala podešena da se za ulaz u operativni sustav koristi zaporka.

- Nastavnici na računalima u svom kabinetu imaju svoje korisničke račune.
- U informatičkim učionicama nastavnici informatike imaju svoje korisničke račune, ali postavljen je i korisnički račun Guest/Korisnik za ostale nasatvnike koje će eventualno koristiti informatičku učionicu.
- Administrativno osoblje, ravnatelj, pedagoginja, psihologinja, voditelji gimnazije, ekonomije i industrijsko – obrtničke škole, satničar i koordinatorica državne mature u svojim uredima koriste računalo koje je zaštićeno zaporkom.

Također je uključena opcija u operativnom sustavu da lozinka ostaje zapamćena (Password never expires).

Preporučuje se korištenje korisničkih zaporki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 8 znakova.

Članak 22.

Odlukom Ministarstva znanosti i obrazovanja prema kojoj se sve osnovne i srednje škole spojene na CARNET-ovu mrežu automatski su uključene u sustav filtriranja nepoćudnih sadržaja. U našem mrežnom sustavu dodatno je uključeno blokiranje pristupa P2P (peer to peer) mrežnom servisu za razmjenu podataka te web stranicama koje podržavaju P2P razmjenu podataka.

Članak 23.

Učenici su upoznati s informacijama o sustavu, odnosno da je sustav podešen tako da filtrira nepoćudan sadržaj, što im se posebno naglašava te se o istome educiraju i upućuju na nastavi informatike. Od učenika se očekuje da prihvate filtriranje određenih sadržaja kao sigurnosnu mjeru te ga ne smiju pokušati zaobići, jer je ono postavljeno radi njihove sigurnosti, ali i sigurnosti svih drugih učenika.

Zaobilaženje sigurnosnih postavki moglo bi ugroziti održavanje nastave. Ako učenik smatra da je određeni sadržaj neopravdano blokiran ili propušten, može se obratiti nastavniku informatike.

Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti nastavnike ili ravnatelja

Članak 24.

U Školi postoji nadzor mrežnog prometa putem Meraki Cloud System od strane e-tehničara Škole.

V. Sigurnost korisnika

Članak 25.

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

Članak 26.

Za sva računala i programe koji zahtijevaju prijavu, mora se posebno voditi računa da se kod prijave ne otkriju podatci za prijavu. Isto tako se učitelji, kada odlaze iz učionice, a ostavljaju računalo uključeno, obavezno moraju odjaviti iz svih sustava u koje su se prijavili. Ukoliko učenici koriste računala u STEM učionicama, obavezno se nakon završetka rada moraju odjaviti iz sustava u koje su se prijavili. Učenici, nastavnici i ostali djelatnici moraju posebno voditi računa o svom digitalnom identitetu koji su dobili iz sustava AAI@edu. Svoje podatke moraju čuvati.

Članak 27.

Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjskog diska, ili interneta) mogu ugroziti sigurnost učenika, odnosno nastavnika. Uputno je ne otvarati ili prosljeđivati zaražene datoteke i programe kao niti otvarati datoteke iz sumnjivih ili nepoznatih izvora. Sve takve datoteke potrebno je provjeriti antivirusnim alatom prije korištenja.

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

Članak 28.

Svi učenici, nastavnici te ostalo osoblje Škole posjeduju elektronički identitet u sustavu AAI@Edu.hr. U školi se često izvodi revidencija korisničkih računa. Svi učenici dobivaju elektronički identitet ispisan u analognom obliku koji im se daje na čuvanje i korištenje. U slučaju gubitka korisničke oznake ili zaporke, odnosno u slučaju da mu je zaključan elektronički identitet, učenik ili roditelj treba se javiti administratoru imenika te mu se ispisuje korisnički račun s novom lozinkom.

U slučaju da učenik seli iz naše u neku drugu Školu, njegov se eletronički identitet privremeno briše. U slučaju da učenik iz neke Škole dolazi u našu, njegov se elektronički identitet prenosi.

Isto vrijedi i za nastavnike i ostalo osoblje.

Minimalno jednom godišnje (početkom školske godine) potrebno je revidirati elektroničke identitete učenika. Pri zapošljavanju novog djelatnika administrator imenika dodjeljuje mu elektronički identitet u sustavu AAI@EduHr, a pri prestanku radnog odnosa, identitet je potrebno zatvoriti.

Članak 29.

Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno zatvoriti. Nastavnicima i ostalom osoblju prava pristupa računalnoj mreži prestaju odlaskom u mirovinu ili prestankom rada u školskom sustavu.

Članak 30.

Pravila pristupa učenika i djelatnika Škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati.

Prihvatljivo i odgovorno korištenje informacijsko-komunikacijske tehnologije.

Ponašanje na internetu

Članak 31.

Korisnici školskih računala odgovorni su za svoje ponašanje u virtualnom svijetu. Moraju se ponašati pristojno prema drugim korisnicima - ne vrijeđati ih i ne objavljivati neprimjerene sadržaje.

Svakog korisnika koji se susreće s internetom nužno je prvo upoznati s osnovnim pravilima ponašanja u takvoj komunikaciji i takvom okruženju., odnosno s 'internetskim bontonom' koji se često naziva i 'Netiquette'. To je ustaljen popis pravila lijepog ponašanja u internetskoj komunikaciji koji je preveden na mnoštvo jezika. Hrvatske stranice dostupne su na http://hr-netiquette.org. 'Netiquette' propisuje smjernice i pravila ponašanja u tri kategorije: elektronička pošta, popis e-adresa i forumi.

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

Članak 32.

Na satu razrednika ili satu informatike učenike će se poučiti da na internetu ne otkrivaju osobne podatke što uključuje adresu, ime škole, telefonske brojeve i slično.

Članak 33.

U učionicama informatike, na oglasnoj ploči u holu Škole te na web stranicama Škole bit će izvješena Pravila sigurnog ponašanja koja sadrže naputke:

- Na internetu se ne smiju odavati osobne informacije.
- Zaporka je tajna, ne smije se nikome odati.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke!
- U slučaju da doživite zlostavljanje na internetu, obavijestite razrednika ili drugu odraslu osobu.
- Treba pomoći prijateljima koji su zlostavljanji putem interneta tako da se to ne prikriva - odmah obavijestiti odraslu osobu (razrednika, predmetnog profesora,…).
- Provjerite na društvenim mrežama koje koristite je li vaš profil skriven za osobe koje vam nisu "prijatelji".
- Pripazite koje osobe prihvaćate za "prijatelje" na društvenim mrežama.
- Budite oprezni s izborom fotografija koje objavljujete na društvenim mrežama
- Provjerite postoji li neka mrežna stranica o vama te koje informacije o vama sadrži (treba upisati svoje ime i prezime u tražilicu).

Autorsko pravo

Članak 34.

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (više na: https://creativecommons.org/licenses/?lang=hr). To je 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, u nekomercijalne svrhe. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Korisnike (profesore, učenike,…) se potiče da materijale koje su izradili potpišu nekom od licenca. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove niti nedopušteno preuzimati tuđe radove s interneta. Svako korištenje tuđih materijala s interneta mora biti citirano pri ćemu treba navesti autora materijala i izvor informacija (poveznica i datum preuzimanja).

Članak 35.

Računalni programi također su, kao i jezična djela, zaštićeni zakonom. 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.

Članak 36.

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

Dijeljenje datoteka

Članak 37.

Pri korištenju digitalnih sadržaja, a osobito pri njihovu dijeljenju treba biti osobito oprezan.

Dijeljenje datoteka samo po sebi nije nelegalno. U slučaju da je datoteka proizvod pojedinca, pojedinac je može podijeliti s drugima na različite načine. Pritom je uputno zaštititi djelo nekom vrstom prikladne licence.

Primjer nelegalnog dijeljenja datoteke jest kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili videosadržaja. 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, glazbeni sadržaji, ključevi za korištenje različitih aplikacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, koja izričito zabranjuju daljnje distribuiranje i umnožavanje bez dopuštenja 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 što je također nelegalno.

U Školi se izričito zabranjuje nelegalno kopiranje ili preuzimanje autorski zaštićenog materijala. 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. Torrent klijenti će se moći instalirati i pokrenuti, ali neće moći ostvariti nikakav mrežni promet.

Obveze ustanove su informirati, usmjeriti i podučiti učenike i nastavnike o:

- autorskom pravu i intelektualnom vlasništvu
- korištenju licenci za zaštitu autorskog prava i intelektualnog vlasništva - mogu se koristiti materijali s https://creativecommons.org/licenses/?lang=hr
- 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.
- mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Internetsko nasilje

Članak 38.

Internetsko nasilje namjerno je i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja. Nasilje putem interneta, u svijetu poznato kao cyberbullying, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro. Postoje različiti oblici internetskog zlostavljanja:

- nastavljanja 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 putem 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 39.

Nedopušteni su svi oblici nasilničkog ponašanja, stoga će svi oni za koje se utvrdi da provode takve aktivnosti biti sankcionirani u skladu s Pravilnikom o pedagoškim mjerama i Kućnim redom Škole.

Edukacije o neprihvatljivom ponašanju provode se kroz predmete koji koriste tehnologiju ili Sat razrednika. Pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva su i u prostorijama Škole.

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

Učenike i nastavnike potrebno je poučiti o mogućim oblicima internetskog nasilja kao i o tome kako ga prepoznati.

Članak 40.

U Školi je potrebno razviti nultu stopu tolerancije na internetsko nasilje.

Škola se obvezuje da će:

- podučiti učenike i nastavnike o mogućim oblicima i kako prepoznati internetsko nasilje
- jasno istaknuti prihvatljiva pravila ponašanja
- izraditi strategiju odgovora na internetsko nasilje
- razviti 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 se potaknula svijest o temi među učenicima).

Korištenje mobilnih telefona

Članak 41.

Kućnim redom Škole propisano je da je zabranjeno korištenje mobitela za vrijeme nastave. Učenik koji, korištenjem mobitela za vrijeme nastave, koje nije odobrio odgojno-obrazovni radnik, ometa odgojno-obrazovni rad, obvezan je predati mobitel odgojno-obrazovnom radniku koji će ga vratiti učeniku na kraju nastavnoga sata. Učenici mogu koristiti mobitel u slobodno vrijeme (mali odmor, veliki odmor) poštujući odredbe Pravilnika i Kućnog reda. Iznimno, učenici mogu korisiti 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. Cilj uporabe svake mobilne tehnologije u učionici mora biti učenje novih ili ponavljanje stečenih sadržaja na nov i učenicima zanimljiv način.
Sigurnosne mjere za korištenje interneta računalom važne su i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama, i slično).
Škola će upoznati učenike s posljedicama zlouporabe mobilnih telefona. Zlouporaba uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti (tekstualna poruka, videoporuka, fotografija, poziv), odnosno kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Ovaj Pravilnik stupa na snagu danom donošenja.

KLASA: 003-05/18-01/1.

URBROJ: 2149-11-01-18-01.

Našice, 12.travnja 2018.

PREDSJEDNICA ŠKOLSKOG ODBORA:

Tomislava Špehar, prof.