Na temelju 24. članka Statuta OŠ Sveti Križ Začretje, Školski odbor na 5. sjednici održanoj 02.11.2017. donosi:

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OSNOVNE ŠKOLE SVETI KRIŽ ZAČRETJE

OPĆE ODREDBE

Članak 1.

Ovaj Pravilnik jasno i nedvosmisleno određuje načine prihvatljivog i dopuštenog korištenja IKT resursa Škole.

Pravilnik vrijedi za sve korisnike IKT infrastrukture Škole i CARNET-ove mreže

Učenici i drugi korisnici prostora škole obvezni su pridržavati se uputa koje će dobiti od učitelja, tajnice, stručne službe, e–tehničara, administratora sustava i ravnatelja, a kojima je cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

Uputa koje će dobiti od školskog administratora sustava o korištenju školske informatičke opreme i mreže, obvezni su se pridržavati i svi djelatnici škole.

OSNOVNE SIGURNOSNE ODREDBE

Članak 2.

Izuzetno je važna sigurnost informacija, infrastrukture te utjecaj ljudskih i drugih resursa na funkcionalnost pojedinih dijelova IKT infrastrukture.

U školi je cjelokupno mrežno rješenje bazirano na opremi proizvođača Cisco Systems, odnosno Cisco meraki rješenje zasnovano na upravljanju sustavom putem oblaka.

U školi je implementiran integrirani sigurnosni sustav, a mrežnom opremom u školi upravlja se putem Cisco Meraki Dashboarda, odnosno središnjeg sustava za upravljanje i nadzor mreže, smještenog u oblaku.

U Cisco Meraki mrežnom rješenju, sustav za upravljanje i nadzor mreže, odnosno Meraki dashboard, jest središnja mrežna komponenta, dok mrežni uređaji imaju funkciju odrađivanja funkcionalnosti i konfiguracije koju dobivaju od Meraki dashboarda.

Sustav za nadzor i upravljanje je nužna komponenta sustava, budući da konfiguracija Meraki mrežne opreme nije moguća niti na jedan drugi način, osim kroz Meraki dashboard.

Meraki dashboard je centralizirano web administratorsko sučelje, izrazito intuitivno i jednostavno za korištenje IT administratorima.

Korisnici IKT infrastrukture u školi su učenici i djelatnici škole.

Školsku opremu je potrebno čuvati i koristiti pažljivo.

Tuđi osobni podaci se mogu koristiti isključivo uz prethodno odobrenje.

U školi se koriste antivirusni programi, vatrozid te sigurnosna kopija podataka osobno kod učitelja i ostalih djelatnika u svrhu sigurnosnih mjera zaštite podataka.

Zaposlenici su dužni koristiti službenu e-mail adresu (ime.prezime@skole.hr) za komunikaciju, posebice u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

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

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

Škola sankcionira kršenje/nepridržavanje pravila u skladu sa službenim aktima škole.

Svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se e-škole tehničaru , e-dnevnik administratoru ili ravnatelju škole.

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

ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 3.

U školi postoji lokalna računalna mreža i to u žičanom i bežičnom obliku.

U školi postoje sveukupno 22 pristupne točke za bežični internet.

Osim mreže, dvije učionice su opremljene monitorima osjetljivima na dodir te videokonferencijskom opremom.

Jedna učionica opremljena je tabletima i kolicima za punjenje tableta.

Učitelji STEM predmeta opremljeni su hibridnim računalima, a svi ostali učitelji u matičnoj školi tabletima, dok su učitelji u područnim školama i stručni suradnici opremljeni prijenosnim računalima.

Naknadno je još jedna učionica opremljena tabletima i kolicima za punjenje tableta.

Knjižnica i PŠ Mirkovec su opremljene pametnim pločama.

Informatička učionica je opremljena s 22 računala.

Računalne mreže te oprema iz projekta e-škole održavaju se preko tehničara e-škole u nadležnosti Carneta, dok se informatička učionica održava isključivo samostalno.

Računalni otpad škole zbrinjava se u skladu sa zakonom.

Svaka učionica u školi ima žičani i bežični pristup internetu, a dodatni žičani pristup imaju knjižnica, zbornica te uredi administrativnog osoblja.

Bežična mreža dostupna je u svakom dijelu školske zgrade, a učenici i djelatnici se mogu spojiti preko tri različita SSID-a (Service Set Identifier), odnosno 3 različite bežične mreže: eSkole, eduroam i guest. ESkole bežična mreža se koristi za spajanje tableta u STEM učionicama. Korisnici koji imaju AAI@EduHr identitet spajaju se na eduroam mrežu, a svi ostali na guest mrežu.

Instalirani sustavski programi na školskim računalima isključivo su preuzeti s Microsoft Download Centra (MSDC) kao središnjeg centra za preuzimanje sustavskih i aplikativnih programa u RH za potrebe osnovnih i srednjih škola.

Na istom mjestu su preuzeti i ključevi za njihovo korištenje.

Nadzor licenciranja sustavskih i aplikativnih programa koji se koriste u školi je isključivo preko MSDC sustava.

Instalaciju i održavanje računalnih programa provodi učitelj informatike, e-tehničar i e-dnevnik administrator.

Učenici ne smiju sami instalirati programe na računala. Ako za to postoji potreba, javiti se učitelju informatike, e-tehničaru i e-dnevnik administratoru.

Za nepridržavanje pravila za instaliranje programa postoje sankcije propisane službenim aktima škole.

REGULIRANJE PRISTUPA IKT OPREMI

Članak 4.

Kako bi se zaštitila materijalna (IKT oprema) i nematerijalna imovina (informacije i podaci), reguliran je pristup svim IKT resursima.

Računalnoj mreži u školi mogu pristupiti djelatnici i učenici škole te svi ostali koji imaju za to dopuštenje.

Bežičnoj mreži se pristupa isključivo preko AAI@EduHr, tj. preko elektroničkog identiteta.

Elektronički identitet u sustavu AAI@EduHr je virtualni identitet na CARNet mreži koji dobivaju pojedinačni korisnici iz ustanova članica CARNeta (učenici, nastavnici, studenti, profesori i zaposlenici ustanova članica), a koji im omogućuje korištenje CARNetovih usluga.

U školi je instaliran Meraki MX vatrozid koji sadrži velik broj sigurnosnih mogućnosti: od klasičnih funkcionalnosti L3/L4 vatrozida, naprednih (next-gen) funkcionalnosti vatrozida, IPS-a, do mrežnog antivirusa. Osim toga sadrži i mogućnosti klasičnog, tzv. border gateway uređaja namijenjenog za pozicioniranje na perimetru lokalne mreže prema internetu.

Na Meraki MX UTM-u je uključen i IPS (Intrusion Prevention System) modul koji štiti mrežu od različitih napada s Interneta kao i sustav za otkrivanje i blokiranje nepoželjnog Malware-a.

U sklopu Meraki mrežnog rješenja integrirano je i MDM rješenje, odnosno sustav za upravljanje klijentskim uređajima kroz Meraki centralizirano web sučelje. Navedeno rješenje omogućuje upravljanje, dijagnostiku i nadzor nad sigurnosnim postavkama klijentske opreme s IOS, android, Windows phone, Windows, Windows Server i MacOS operativnim sustavima.

Osim filtriranja sadržaja, moguće je blokirati pristup pojedinim mrežama korištenjem klasičnih Layer 3 i Layer 7 pristupnih listi (ACL – Access Control List).

Za svaki VLAN konfiguriran na mreži podignut je DHCP server na Meraki MX UTM uređaju. U pravilu, vrijeme čuvanja IP adrese pojedinom klijentu (Lease time) je 4 sata za VLAN-ove koji se koriste i za bežične klijente te 24 sata za VLAN-ove koji se koriste samo za spajanje žičnih klijenata.

Za pristup mreži eSkole 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

• 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 koriste se sljedeći parametri:

• 802.1X enterprise RADIUS autentikacija, uz WPA2 enkripciju podataka

• za pristup mreži eduroam koriste se postavke TTLS-PAP

• 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 nastavnicima koji tada pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23

• za navedenu mrežu se limitira ukupna propusnost na 10% ukupne propusnosti internetske veze, ako se ne radi o nastavnicima, odnosno ako se klijenti pozicioniraju u VLAN 14.

Za pristup guest mreži koriste se sljedeći parametri:

• otvoren pristup mreži, uz mogućnost Captive portal autentikacije pristupa na internet

• za autentikaciju se koristi baza korisnika iz Meraki dashboarda

• korisnici nakon pristupa u mrežu eduroam pripadaju u VLAN 13 i imaju IP adresu iz mreže 192.168.36.0/23

• za navedenu mrežu se limitira ukupna propusnost na 10% ukupne propusnosti veze prema internetu.

Preko besplatne Office365 usluge i alata koji omogućuju suradnju i komunikaciju između svih sudionika u obrazovnom sustavu, moguće je koristiti i OneDrive kao način za pohranjivanje sadržaja na oblak. Pristup OneDrive-u za škole moguć je preko AAI@EduHr elektroničkog identiteta.

Računala u informatičkoj učionici se koriste za vrijeme trajanja nastave informatike te ih u to vrijeme koriste učenici. Ostala računala u školi učenici smiju koristiti za vrijeme odmora.

Korištenje opreme u informatičkoj učionici propisano je posebnim pravilima kojih se učenici moraju pridržavati, a nepridržavanje navedenih pravila sankcionira se u skladu sa službenim aktima škole.

Zaporke koje koriste učenici i ostali djelatnici moraju sadržavati brojke i slova te minimalno 8 znamenki.

U školi se provodi filtriranje nepoćudnih sadržaja. Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNet mrežu automatski su uključene i u sustav filtriranja nepoćudnih sadržaja. Odlukom MZO-a onemogućava se prikazivanje 14 kategorija stranica na računalima u osnovnim i srednjim školama.

Učenici su obvezni prihvatiti 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. Zabranjeno je zaobilaženje bilo kojih sigurnosnih postavki računalne opreme.

EDUKACIJA

Članak 5.

Da bi se održao korak s trendovima u korištenju IKT-a, kao i s nadolazećim prijetnjama računalnoj sigurnosti, obvezna je stalna edukacija učenika i cijelog školskog kolektiva.

Učenici se prijavljuju na računala kao standardni korisnici, a učitelji kao administratori.

Zabranjuje se ophođenje s privatnim (i tajnim) podacima koje su korisnici dobili od škole (poput elektroničkog identiteta u sustavu AAI@Edu.hr i sl.).

Preuzimanje datoteka na lokalno računalo i moguće pokretanje izvršnih datoteka mora biti uz dopuštenje učitelja.

Elektronički identitet u sustavu AAI@EduHr ima oblik ID_korisnika@oznaka_ustanove.hr

Elektronički identitet u sustavu AAI@Edu.hr dodjeljuje administrator elektroničkog (LDAP) imenika škole.

Učeniku prestaju prava za korištenje AAI@Edu.hr identiteta završetkom školovanja, a djelatnicima prestankom rada u ustanovi.

PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Članak 6.

6.1.Ponašanje na internetu

Za svakog korisnika koji se susreće s internetom nužno je prvo upoznati ga 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. 'Netiquette' propisuju smjernice i pravila ponašanja u tri (3) kategorije: elektronička pošta, popis e-adresa i forumi. Poželjno je da škola ovaj skup pravila učini dostupnim svojim učenicima, o tome ih poduči te primijeni vlastitu politiku u skladu s tim pravilima.

'Netiquette' će biti izvješena u informatičkoj učionici.

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

Učenici se uz Pravila lijepog ponašanja na internetu moraju pridržavati i Pravila sigurnog ponašanja, koja uključuju naputke poput:

- Osobne se informacije na internetu **nikad** ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke!
- Obveza je pomoći prijateljima koji su zlostavljani preko interneta tako da se to ne prikriva i da se odmah obavijeste odrasli.
- Provjeriti je li Facebook profil skriven za osobe koji nam nisu ‘prijatelji’. Treba biti kritičan prema ljudima koji se primaju za ‘prijatelje’.

- Potrebno je biti oprezan s izborom fotografija koje se objavljuju na Facebooku.

Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

6.2 Autorsko pravo

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (vidite: https://creativecommons.org/licenses/?lang=hr). Creative Commons licence jesu skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Svaka od licenci pomaže autorima zadržavanje svojih autorskih prava, a drugima dopušta umnožavaje, distribuiranje i na neke druge načine korištenje njihovih djela, barem u nekomercijalne svrhe. Svaka Creative Commons licenca osigurava davateljima licence, priznavanje i označavanje kao autore djela.

Učenici i djelatnici moraju potpisati materijale koje su sami izradili koristeći neku licencu, ali i poštivati tuđe radove. Zabranjuje se: tuđe radove predstavljati kao svoje, preuzimanje zasluga za tuđe radove i nedopušteno preuzimanje tuđih radova s interneta. Korištenje tuđih materijala s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Pri korištenju IKT opreme važno je napomenuti i da su računalni programi također zaštićeni zakonom kao jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju. U to su uključeni naravno i mrežni programi, odnosno aplikacije.

Kod mrežnog mjesta je moguće 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.

6.3. Dijeljenje datoteka

Prednost digitalnog sadržaja je da se ne uništava ili mu se ne umanjuje kvaliteta s brojem kopiranja. Ipak, baš zbog tog vida 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 prikladnom licencom.

Primjer nelegalnog dijeljenja datoteke jest kopiranje ili preuzimanje autorski zaštićenog materijala, poput e-knjige, glazbe ili pak 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 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.

Izričito se zabranjuje nelegalno dijeljenje datoteka.

6.4 Internetsko nasilje

Internetsko nasilje se općenito može definirati kao namjerno i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja.

Postoje različiti oblici internetskog zlostavljanja:

- nastavljanje slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem
- 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.

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

Iako se velika većina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanja djece savjetniku i sl.), postoje i situacije kad se zahtijeva službena reakcija škole.

To se događa u slučajevima koji uključuju ozbiljne prijetnje prema drugim učenicima, a rezultiraju time da žrtva više ne želi ići u školu ili pak ako se nasilje nastavi, iako su već korištena druga neformalna sredstva.

U takvim težim oblicima zlostavljanja potrebno je izreći neku od disciplinskih mjera škole.

Jasne poruke o takvom ponašanju šalju se kroz predmete koji koriste tehnologiju ili Sat razrednika.

Pravila o prihvatljivom ponašanju i korištenju tehnologije trebaju biti vidljiva u prostorijama škole.

6.5 Korištenje mobilnih telefona

U školi je zabranjeno korištenje mobilnih uređaja, osim ako učitelj isto ne dozvoli u svrhu izvođenja nastavnog procesa.

Mobilni uređaji sve više imaju potpuni pristup internetu te djeca i mladi koriste fiksne internetske veze kao i mobitele za pretraživanje interneta. Stoga, iste sigurnosne mjere za korištenje interneta postaju važne i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama)

PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 7.

Ovaj Pravilnik stupa na snagu danom donošenja.

Klasa: 021-03/17-01/24

Urbroj: 2197/04-380-26-17-1

Sveti Križ Začretje, 02. 11. 2017.

PREDSJEDNIK ŠKOLSKOG ODBORA

NIKOLINA MAJSEC