Gospodarska škola Varaždin

Božene Plazzeriano 4

42 000 Varaždin

PRAVILNIK

O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO – KOMUNIKACIJSKE TEHNOLOGIJE GOSPODARSKE ŠKOLE VARAŽDIN

Varaždin, studeni 2018.

Na temelju odredbe članka 58. Statuta Gospodarske škole Varaždin (KLASA: 003-06/17-01/1, URBROJ: 2186-148-02-17-9), te odredbe članka 118. stavka 2. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (Narodne novine broj 87/08., 86/09., 92/10.,105/10., 90/11., 5/12., 16/12., 86/12., 126/12., 94/13., 152/14., 07/17. i 68/18) Školski odbor Gospodarske škole Varaždin, na prijedlog ravnateljice na sjednici održanoj 7. 11. 2018. godine donosi

PRAVILNIK
o sigurnoj i odgovornoj upotrebi informacijsko - komunikacijske tehnologije
Gospodarske škole Varaždin

I. UVOD

Članak 1.

Pravilnikom o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije Gospodarske škole Varaždin (u daljnjem tekstu Pravilnik) definiraju se prihvatljivi i neprihvatljivi načini ponašanja, raspodjeljuju se zadaci i odgovornosti te propisuju sankcije u slučaju nepridržavanja odredbi Pravilnika s ciljem očuvanja integriteta informacijskog sustava Gospodarske škole Varaždin (u daljnjem tekstu Škole), poticanjem aktivnog i odgovornog sudjelovanja učenika u radu s informacijsko-komunikacijskim tehnologijama te osiguranja nesmetanog djelovanja tog sustava pod pretpostavljenim oblicima prijetnji.

Članak 2.

Odredbe Pravilnika odnose se na sve korisnike informacijsko-komunikacijske infrastrukture; učenike, sve djelatnike škole (nastavnike i ostale djelatnike), sve one koji iz bilo kojeg razloga imaju potrebu za njenim korištenjem (učenici i nastavnici, sudionici natjecanja, sudionici seminara i drugih stručnih usavršavanja i ostali gosti Škole).

Članak 3.

Učenici se moraju pridržavati uputa koje im mogu dati nastavnici kako bi se unaprijedila sigurnost školske informatičke opreme i mreže. Za nepridržavanje uputa nastavnika i odredbi Pravilnika učeniku će se izreći odgovarajuća pedagoška mjera određena Pravilnikom o kriterijima za izricanje pedagoškim mjera i Statutom Gospodarske škole Varaždin.

Svi korisnici informacijsko-komunikacijske infrastrukture moraju se pridržavati uputa koje im može dati školski administrator sustava ili neka druga ovlaštena osoba radi unapređenja sigurnosti školske informatičke opreme i mreže.

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 4.

Informacijsko-komunikacijsku infrastrukturu Gospodarske škole Varaždin čine:

a) **Materijalni resursi**
- stolna i prijenosna računala
- tableti
- projektori
- dokument kamere
- digitalne kamere

- mrežna oprema
- i druga oprema

b) Nematerijalni resursi

- operacijski sustavi Windows i Linux instalirani na računalima Škole
- stolne i mrežne aplikacije:
    - uredske aplikacije paketa MS Office (MS Word, MS Excel, MS Access, MS Outlook, MS Power Point),
    - vježbenički ERP,
    - e-Dnevnik,
    - e-Matica,
    - Vetis
    - Web 2.0 alati (Prezi, Glogster i dr.
    - računovodstvene aplikacije
    - aplikacija Urudžbenog zapisnika i Upisnika predmeta prvog stupnja

Članak 5.

Školska oprema treba se čuvati i koristiti pažljivo.

Članak 6.

U poslovanju Škole koriste se javne i povjerljive informacije. Javne informacije vezane su 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 zakonskim propisima dužna objavljivati i drugo).

Povjerljive informacije su osobni podaci učenika, djelatnika(kontakt podaci osobe,fotografije osobe, i drugo),podaci iz evidencija koje se vode u školskim evidencijama (e-Dnevnik, e-Matica, matične knjige) te informacije koje se smatraju poslovnom tajnom. Osobni podaci se mogu koristiti isključivo sukladno pozitivnopravnim propisima o zaštiti osobnih podataka.

Članak 7.

Škola provodi sigurnosne mjere zaštite podataka izradom automatiziranih sigurnosnih kopija, te mjerama na programskoj razini:

- Zaštita na razini operacijskog sustava
- Zaštita na razini korisničke programske podrške
- Kriptiranje podataka u komunikaciji
- Antivirusni alati
- Antispyware alati
- Zaštitni zid (Firewall)

Članak 8.

Škola primjenjuje sigurnosne mjere zaštite podataka na sljedećim razinama:

1. fizičkoj – IKT oprema se nalazi u posebnoj prostoriji u za to predviđenim serverskim i mrežnim ormarima pod ključem, osiguranom zaštitom od strujnih opterećenja.

2. tehničkoj –povjerljivi podaci iz računovodstva i tajništva, te stručno pedagoške-psihološke službe zaštićeni su lozinkama za pristup, te su ovisno o potrebi zaštićeni i enkripcijom.
3. organizacijskoj – samo ovlaštene osobe imaju pristup gore navedenim povjerljivim podacima

Za zaštitu informacijskih sustava GOŠK-a koriste se antivirusni programi (BitDefender, Windows Defender IS360 suite, MalwareByte), vatrozid na središnjem ruteru, Squid proxy (filter) u dijelu računalne mreže pod Optima telekomom kao pružateljem usluge pristupa internetu, CARNET proxy filtar u dijelu računalne mreže pod nadzorom CARNET-a, domenske politike na više razina upravljane Windows Server OS-om, sigurnosne kopija podataka i slike sustava sa servera Gospodarske škole Varaždin i slike sustava računala iz učionica, te sigurnosne kopija podataka iz računovodstva, tajništva i stručno pedagoško-psihološke službe.

Pravila vezana uz sigurnosne mjere zaštite informacijsko-komunikacijske tehnologije:

- nemogućnost korištenja USB memorije,
- nemogućnost izvršavanja power shell skripti,batch skripti, manipulacije .reg datotekama
- nemogućnost samovoljnog instaliranja softvera koji nije u skladu s sigurnosnom politikom škole
- pristup internetu samo preko portova 80,443
- mrežno filtriranje torrenta na središnjem ruteru
- praćenja prometa putem tcp i udp protokola na središnjem ruteru te vođenja zapisnika, prema potrebi blokiranje određenih portova aplikacija zbog neuobičajeno velikog prometa između klijentskih računala i interneta zbog dijagnostike i otklanjanja sigurnosnih prijetnji.

Članak 9.

Nastavnici i djelatnici posjeduju AAI@Edu elektronički identitet te su u svrhu službene komunikacije dužni koristiti službenu e-mail adresu (ime.prezime@skole.hr).

U službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja Škola treba koristiti isključivo službenu adresu elektroničke pošte gospodarska@ss-gospodarska-vz.skole.hr.

Članak 10.

Nastavnicima i drugim djelatnicima Škole strogo je zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i digitalne identitete. To se odnosi na pristup školskim računalima e-Matici, e-Dnevniku, Vetisu, računovodstvenim aplikacijama, knjižničarskim aplikacijama i ostalim informacijskim sustavima ili mrežnim aplikacijama koje sadrže osobne podatke djelatnika i/ili učenika.

Članak 11.

Svi djelatnici Škole moraju se pridržavati etičkih načela pri korištenju informacijsko-komunikacijske tehnologije.

Svako nepridržavanje ovih pravila 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 INFORMACIJSKO-KOMUNIKACIJSKA OPREMA I ODRŽAVANJE

Članak 12.

Računala u školi su povezana bežično i žično. Računalna mreža se sastoji od dva segmenta. Prvi segment spaja se na Internet putem infrastrukture Optima Telekoma (VOIP+Internet), a drugi dio se spaja preko Carneta i njihove infrastrukturne opreme. Bežična mreža koristi Carnet-ovu infrastrukturu za spajanje na Internet.

Administrator mrežnog sustava škole je ovlašteni djelatnik Škole koji je zadužen za održavanje navedene mrežne infrastrukture.

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

Članak 13.

U svakoj učionici nalazi se nastavničko računalo koje je žično spojeno na infrastrukturu CARNET-a ili OPTIMA telekoma. Isto vrijedi i za specijalizirane informatičke učionice. WIFI (bežična mreža) dostupna je samo na prvom katu škole (u izgradnji). Prijenosnici se po potrebi spajaju bežično ili žično (ovisno o dostupnosti mrežnih priključaka).

Članak 13. a

Škola koristi pretežno Microsoft Windows i Windows Server sustavsku programsku podršku. Prevladava većinom Windows 7 Professional i Enterprise verzija 32 bitna. Ostatak računala koristi Windows 8.1 Enterprise i Windows 10 Enterprise i Education verzije. Serverska računala koriste Windows Server 2008 R2 i Windows Server 2012 i Ubuntu 16.04 server verziju. Od aplikativnog softvera najzastupljeniji je Microsoft Office 2007 i 2010. Manji dio računala i prijenosnika koriste Microsoft Office 2013 i 2016. Standardni preglednik je Google Chrome reguliran domenskom politikom.

Članak 13. b

Škola koristi licenciranu sustavsku i korisničku programsku podršku tvrtke Microsoft. Na adresi http://msdc.skole.hr nalazi se središnje mjesto za preuzimanje Microsoftovog softvera za osnovne i srednje škole u Republici Hrvatskoj. Ovom uslugom školama se omogućuje preuzimanje datoteka (ISO imagea) aplikacija i operativnih sustava na koje imaju pravo temeljem ugovora Microsoft School Enrollment potpisanog između Microsofta Hrvatska i Ministarstva znanosti i obrazovanja. Pravo pristupa i preuzimanja datoteka imaju samo određeni administratori resursa u školama koji i imaju pristup do aktivacijskih ključeva za programske pakete. Za instalaciju i održavanje računalnih programa brine se administrator mrežnog sustava. Učenicima je onemogućeno instaliranje programa i narušavanje aplikacijskog ekosustava proizvoljnim aplikacijama. Svako kršenje ovih pravila podliježe pedagoškim mjerama za učenike. Prijedlozi za instalaciju aplikacija s edukativnom svrhom od strane učenika i nastavnika podnose se administratoru mrežnih resursa koji nakon testiranja programa na stabilnost na različitim verzijama operativnog sustava Windows odlučuje o stavljanju u produkciju.

Članak 13. c

1. Funkcioniranje WLAN/HotSpot-a ovisi o više fizičkih faktora, kao i o spojenom klijentu. WLAN/HotSpot je sustav bežičnog prijenosa informacija na kojem može doći do pogoršanja i grešaka u funkcioniranju u i vezi, općenito.

2. Prijenos podataka nije enkriptiran niti zaštićen na bilo koji način s obzirom da se radi o mreži otvorenog tipa, te se Škola ne može na bilo koji način smatrati odgovornim za uspostavljanje bilo kakvog sustava zaštite, nadzora ili upravljanja, te ne snosi nikakvu odgovornost za bilo kakvu zloporabu od strane klijenta ili trećih osoba koje se spajaju, ili bi se mogle spojiti na mrežu, uključujući, bez ograničenja, gubitak, krađu i bilo kakvu drugu manipulaciju podataka, neovlašteno prikupljanje osobnih podataka, poslovne ili službene tajne, ili bilo kakvih drugih povjerljivih informacija, kao ni bilo kakvo oštećenje hardvera ili softvera ili bilo kakvih drugih nepovoljnih ili neželjenih posljedica korištenja WLAN/Hotspot-a.

3. Nema garancije za pouzdano funkcioniranje WLAN/HotSpot -a.

4. Korisnik preuzima punu odgovornost da je spojeni sustav (prijenosno računalo, smartphone, tablet ili drugi uređaj), uključujući i operativni sustav i programske aplikacije i bilo kakva prezentacija podataka slobodna od bilo kakvog zlonamjernog koda. U slučaju povrede, korisnik će biti odgovoran za bilo kakvu štetu (izravnu, neizravnu i posljedičnu štetu) do koje bi moglo doći.

5. WLAN/HotSpot nije zaštićen od neovlaštenog praćenja i krađe podataka korisnika i nije osigurana nikakva pouzdana zaštita podataka pohranjenih na sustavu korisnika.

6. Zloporaba WLAN/HotSpot-a u komercijalne, protuzakonite ili kaznene aktivnosti je strogo zabranjena, te se posebno primjera radi navodi prijenos SPAM poruka, prijetnji, opscenog sadržaja, zlostavljanje ili bilo kakve radnje koje bi mogle vrijeđati korisnike ili nanijeti štetu drugim korisnicima ili sustavima, korištenje peer-2-peer mreža ili drugih sustava za učitavanja ili nuđenje sadržaja koji su zaštićeni autorskim pravima.

7. Korisnik snosi punu odgovornost za bilo kakvu štetu (izravnu, neizravnu i posljedičnu) prouzročenu trećima te će naknaditi pružatelju usluge WLAN/HotSpot-a svu štetu i trošak koja bi mu mogla nastati kao posljedica korištenja te usluge od strane korisnika.

IV. REGULIRANJE PRISTUPA INFORMACIJSKO-KOMUNIKACIJSKOJ OPREMI

Članak 14.

Računalnoj mreži mogu pristupiti učenici, nastavnici, ostali djelatnici Škole i gosti Škole.

Pristup bežičnoj računalnoj mreži je zaštićen, a ovisi o tome tko se želi spojiti na mrežu i s kojim razlogom. Zaštićena je WPA2 enkripcijom i RADIUS autorizacijom i autentikacijom za određene vrste korisnika koji pristupaju povjerljivim podacima.

Članak 15.

Računala u specijaliziranim učionicama i nastavnička računala u učionicama i specijaliziranim učionicama podliježu domenskim politikama, ovisno o zahtjevima i potrebama nastavnika. Sve domenske politike onemogućuju proizvoljno instaliranje programa, aktiviraju vatrozid za „surfanje" samo preko portova 40,443, onemogućavaju premošćivanje politika putem „proxy-a", blokiraju upotrebu prijenosnih USB memorija.

Po dogovoru s voditeljima kabineta na poslužitelju se po potrebi uređuju mrežne mape s pravima pristupa ovisno o vrsti podataka koje će se pohranjivati na poslužitelju.

Nastavnici koji koriste opremu u informatičkim učionicama dužni su prije korištenja provjeriti opremu na moguće nedostatke i iste prijaviti administratoru mreže te uputiti učenike da ju pažljivo koriste i ne oštećuju.

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.Odlukom Ministarstva znanosti i obrazovanja, filtrirat će se mrežne stranice koje ulaze u sljedeće kategorije:

- Drugs
- Gambling
- Gambling Related
- Gruesome Content
- Hate Speech
- Hacking
- Malicious Sites
- Nudity
- Profanity
- Pornography
- School Cheating Information
- Spam
- Tobacco
- Violence.

Popis kategorija je na engleskom jeziku zbog njegove raširenosti na internetu, te lakšoj kategorizaciji i stranica s ne-hrvatskog govornog područja.

Učenici korištenjem računalne opreme u vlasništvu Škole prihvaćaju filtriranje sadržaja kao sigurnosnu mjeru, te im nije dozvoljeno zaobilaziti sigurnosne postavke računalne opreme zbog mogućeg narušavanje vlastite, ali i sigurnosti ostalih učenika na internetu.

Nadzor prometa za protokole koje ne filtrira CARNET vrši se na središnjem ruteru od strane mrežnog administratora koji poduzima odgovarajuće radnje u slučaju zlouporabe istih.

Članak 16.

Učenici smiju uz dopuštenje predmetnog nastavnika koristiti samo školska računala koja su njima namijenjena (računala u informatičkoj učionici).

Vlastita računala i pametne telefone učenici smiju za vrijeme nastave koristiti isključivo u obrazovne svrhe i uz prethodnu dozvolu i nadzor nastavnika, pri čemu moraju paziti na odgovorno ponašanje te da ne ugrožavaju druge korisnike školske mreže širenjem virusa i drugih zlonamjernih programa.

Kojim aplikacijama i internetskim sadržaj ima učenici mogu pristupiti određuje isključivo predmetni nastavnik.

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

Članak 17.

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

- Učionica mora ostati na kraju onako kako 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 učionice obavezno zatvoriti
- Učionicu zaključati

Nastavnik i učenici koji koriste informatičku učionicu odgovorni su za opremu instaliranu u njoj.

Članak 18.

Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNet mrežu automatski su uključene i u sustav filtriranja nepoćudnih sadržaja. 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 korisnika.

Zaobilaženje sigurnosnih postavki moglo bi ugroziti održavanje nastave.

Ako učenik smatra da je određeni sadržaj neopravdano blokiran ili propušten može se obratiti predmetnom nastavniku. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti nastavnike ili ravnatelja.

U Školi postoji nadzor mrežnog prometa kroz središnji ruter, a sustav nadzire administrator mreže.

V. SIGURNOST KORISNIKA

Članak 19.

U Školi je potrebna neprekidna edukacija učenika, nastavnika i ostalih djelatnika da bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti. Pri korištenju računala i aplikacija koji zahtijevaju prijavu lozinkom, potrebno je voditi računa da se kod prijave ne otkriju podaci o prijavi.

Kada učenici odlaze iz učionice, a ostave računalo uključeno, nastavnici su dužni odjaviti ih iz svih sustava u koje su se prijavili.

Učenici koji koriste računala za rad u Vježbeničkom ERP-u dužni su se obvezno nakon završetka rada odjaviti iz sustava,

Članak 20.

Korisnici informacijsko komunikacijske tehnologije su dužni posebno voditi računa o svojem elektroničkom identitetu koji su dobili iz sustava AAI@Edu.Svoje podatke moraju čuvati.

Početkom školovanja u Školi svi učenici dobivaju elektronički identitet u sustavu AAI@Edu. U slučaju gubitka korisničke oznake ili zaporke, odnosno u slučaju da mu je zaključan elektronički identitet, učenik se treba javiti administratoru imenika.

Kada učenik prelazi u Školu iz druge škole, njegov elektronički identitet se ne prenosi.

Minimalno jednom godišnje (početkom školske godine) potrebno je revidirati elektroničke identitete učenika.

Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno zatvoriti.

Pri zapošljavanju novog djelatnika, administrator imenika dodjeljuje mu elektronički identitet u sustavu AAI@Edu, a pri prestanku radnog odnosa, identitet je potrebno zatvoriti.

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

Članak 21.

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

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJA

PONAŠANJE NA INTERNETU

Članak 22.

Korisnici školskih računala odgovorni su za svoje ponašanje u virtualnom svijetu te se prema drugim korisnicima moraju ponašati pristojno, ne vrijeđati ih,niti objavljivati neprimjerene sadržaje. Škola će korisnike upoznati s pravilima poželjnog ponašanja na internetu-„Netiquette", objavljivanjem navedenih pravila u informatičkoj učionici.

Članak 23.

Učenike se na nastavi informatike, na nastavni gdje se koriste računala i satu razrednika poučava o osnovnim pravilima ponašanja u virtualnom svijetu (ne otkrivati osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično putem društvenih mreža poput Facebooka, Instagrama, chat sobe...).

Članak 24.

Osim Pravila poželjnog ponašanja na internetu, uputno je da se učenici pridržavaju i naputaka Pravila sigurnog ponašanja na internetu:

- Osobne informacije na internetu se nikad ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke!
- Treba pomoći prijateljima koji su zlostavljani preko interneta tako da se to ne prikriva i da se odmah obavijeste odrasli.
- Treba 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 društvenim mrežama.
- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

Nastavnici trebaju odgovornom i sigurnom upotrebom informacijsko-komunikacijske tehnologije biti primjer učenicima.

AUTORSKO PRAVO

Članak 25.

Korisnike poticati na potpisivanje vlastitih uradaka te na poštivanje autorskih prava tuđih radova.

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, obavezno navodeći ime autora korištenih materijala te izvor (poveznica i datum preuzimanja sadržaja).

Članak 26.

Računalni programi su kao jezična djela također zaštićeni zakonom. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju, a u što su uključeni i on-line programi odnosno web aplikacije.

Članak 27.

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 28.

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

U Školi je izričito zabranjeno nelegalno dijeljenje datoteka kao što je kopiranje ili preuzimanje autorski zaštićenih materijala poput e-knjiga, glazbe ili pak video sadržaja.

Učenike i nastavnike treba podučiti o autorskom pravu i intelektualnom vlasništvu te ih usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva.

Učenike i nastavnike treba podučiti o načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju (npr. Torrent).

Učenike i nastavnike treba informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

INTERNETSKO NASILJE

Članak 29.

Internetsko nasilje se općenito definira 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-pošte i drugih servisa za komunikaciju),
- postavljanje internetske ankete o žrtvi,
- slanje virusa na e-mail ili mobitel,
- slanje uznemirujućih fotografija putem e-pošte, MMS-a ili drugih komunikacijskih alata

Članak 30.

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

Potrebno je sve korisnike informacijsko-komunikacijske tehnologije u Školi poučiti o mogućim oblicima internetskog nasilja te o tome kako prepoznati internetsko nasilje.

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

KORIŠTENJE MOBILNIH TELEFONA

Članak 31.

Kućnim redom Škole (članak 25.) određeno je da se mobilni telefoni, računala i ostali tehnički aparati ne smiju koristiti za vrijeme nastave, osim uz odobrenje i nadzor predmetnog nastavnika.

Iznimno,učenici mogu koristiti mobilne telefone za vrijeme nastave, kada predmetni nastavnik to zatraži i pravovremeno najavi. Učenici mogu u Školi koristiti mobilne telefone za vrijeme odmora, prije ili poslije nastave, poštujući odredbe Kućnog reda Škole i ovog Pravilnika.

Kako mobilni telefoni sve više imaju potpuni pristup internetu a djeca i mladi koriste i fiksne internetske veze kao i mobitele za pretraživanje interneta korisnike informacijsko-komunikacijske infrastrukture u Školi je potrebno osvijestiti o važnosti sigurnosnih mjera za korištenje interneta i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama, i slično) i o posljedicama zlouporabe mobilnih telefona.

Najraširenij oblik nasilja među vršnjacima je nasilje putem mobilnih telefona. Ono uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti

VII. ZAVRŠNE ODREDBE

Članak 32.

Ovaj Pravilnik objavljuje se na oglasnoj ploči Škole i službenoj mrežnoj stranici Škole, a stupa na osmoga dana od dana njegove objave na oglasnoj ploči Škole.

"GOSPODARSKA ŠKOLA" VARAŽDIN

Predsjednik Školskog odbora:

Tomislav Purgarić, dipl. inf.

KLASA: 003-06/18-01/1

URBROJ: 2186-148-02-18-11

Varaždin, 7. 11. 2018. godine.

Ovaj Pravilnik objavljen je na oglasnoj ploči Škole 7. 11. 2018. godine, a stupa na snagu 15. 11. 2018. godine.

"GOSPODARSKA ŠKOLA" VARAŽDIN

Ravnateljica Škole:

Katica Kalogjera Novak, dipl. ing