



**REPUBLIKA HRVATSKA  
GRAD ZAGREB  
OSNOVNA ŠKOLA ODRA  
Zagreb, Đačka 5**

Temeljem članka 57. Statuta Osnovne škole Odra, dana 29.01.2019. ravnatelj Osnovne škole Odra uz suglasnost Učiteljskog vijeća, donosi

**PRAVILNIK  
O PRIHVATLJIVOM KORIŠTENJU RAČUNALNIH RESURSA**

**OSNOVNE ODREDBE**

**I.**

- 1) Pravilnikom o prihvatljivom korištenju računalnih resursa Osnovne škole Odra (u daljnjem tekstu: Pravilnik) uređuju se osnovne sigurnosne odredbe, informacijsko-komunikacijska tehnologija ( u daljnjem tekstu: IKT) i njezino održavanje te uvjeti prihvatljivog i odgovornog korištenja IKT opreme Osnovne škole Odra.
- 2) Svrha je ovog Pravilnika jasno određivanje načina dopuštenog i prihvatljivog korištenja računalnih resursa Osnovne škole Odra (u daljnjem tekstu: škola).
- 3) Cilj je ovog Pravilnika povećanje sigurnosti rada i učenja u školi.

**OPĆE SIGURNOSNE ODREDBE**

**Korisnici**

**II.**

- 1) Korisnici računalnih resursa škole jesu radnici, učenici, vanjski suradnici za održavanje i svaka druga osoba koja uz odobrenje škole koristi računalne resurse škole.
- 2) Radnici se moraju pridržavati uputa koje im daju školski administratori sustava ili druge ovlaštene osobe. Učenici se moraju pridržavati i drugih uputa koje im mogu dati učitelji,, a koje imaju za cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

- 3) Svako nepridržavanje ovih pravila ima negativan utjecaj za školu i može rezultirati disciplinskim mjerama prema radnicima ili pedagoškim mjerama prema učenicima, odnosno pokretanjem odgovarajućih postupaka prema trećim osobama u skladu s važećim propisima.
- 4) Obveza je škole osigurati da se na području njene odgovornosti korisnici ponašaju u skladu s odredbama Odluke o prihvatljivom korištenju CARNet mreže.
- 5) Svatko je dužan ponašanje protivno ovom Pravilniku prijaviti odgovornoj osobi (učitelju, administratoru resursa ili ravnatelju.)

## **IKT INFRASTRUKTURA**

### **III.**

- 1) IKT infrastrukturu čine fiksna i bežična mreža sa svim svojim mrežnim uređajima, sva školska stolna, prijenosna i tablet računala te ulazno-izlazni uređaji bez obzira jesu li vlasništvo škole ili se škola služi tim uređajima.
- 2) IKT infrastruktura mora omogućavati neometan pristup i korištenje informacijama potrebnih u nastavi i drugim aktivnostima vezanim za rad škole.
- 3) Korisnici ne smiju uništavati IKT infrastrukturu škole. Svaki radnik pri preuzimanju opreme na korištenje potpisuje zadužnicu kojom se obvezuje po prestanku korištenja vratiti opremu u ispravnom stanju, a u suprotnom odgovara za nastalu štetu.

## **SIGURNOST INFORMACIJA**

### **IV.**

- 1) Načelo povjerljivosti informacija podrazumijeva da informacije moraju biti dostupne samo onome kome su namijenjene. U skladu s ovim načelom škola razlikuje javne i interne informacije.
- 2) Skupinu javnih informacija čine one informacije koje opisuju djelatnosti škole, a njihova javna dostupnost je u interesu škole, kao na primjer sadržaji i podaci koje je škola dužna objavljivati na svojim mrežnim stranicama, informacije o aktivnostima škole i slično.
- 3) Interne informacije su one informacije koje se odnose na osobne podatke pojedinaca (npr. kontakt podaci osobe, fotografije osobe, podaci iz evidencija koje vodi škola - Razredna knjiga, matične knjige) te informacije koje su namijenjene samo djelatnicima škole. Tuđe osobne podatke zabranjeno je koristiti bez dopuštenja osobe odgovorne za te podatke.
- 4) Poslovnu dokumentaciju važnu za poslovanje Škole, održavanje nastave te druge važne dokumente je potrebno čuvati na zakonom propisani način.

- 5) Sigurnosna preslika je kopija informacija na drugom računalu. Kako bi se spriječilo nepovratno oštećenje ili gubitak informacija, za sve informacije koje se pohranjuju na računalima škole, a za koje škola procijeni da su važne potrebno je redovito izrađivati njihovu sigurnosnu presliku. Svaki je radnik odgovoran za izrađivanje preslika svojih podataka.
- 6) Mjere fizičke sigurnosti primjenjuju se na sva mjesta gdje se nalaze podaci važni za rad škole, uz primjenu važećih propisa, tehničkih pravila i pravila struke.
- 7) Svi radnici dužni su u poslovnoj komunikaciji koristiti se službenom elektroničkom adresom (@skole.hr) te ne smiju vlastite elektroničke identitete i pripadajuće lozinke davati učenicima ili drugim osobama. To se odnosi na personalizirani pristup računalu, matici podataka Grada Zagreba, e- matici Ministarstva znanosti i obrazovanja, e- Dnevniku, bazi za upise u srednje škole, računovodstvenim programima, knjižničarskim programima i ostalim programima ili mrežnim aplikacijama koje sadrže osobne podatke radnika i /ili učenika. Za pristup bežičnoj mreži korisnici škole upotrebljavaju AAI@EduHr ( skole.hr) identitet.
- 8) Radnici i vanjski suradnici koji zbog prirode svog posla imaju pristup osobnim podacima ostalih osoba dužni su pridržavati se svih važećih propisa i etičkih načela iz područja zaštite osobnih podataka te na zahtjev škole o tome potpisati izjavu o tajnosti podataka.

## **ŠKOLSKA IKT OPREMA I ODRŽAVANJE**

### **Školske računalne mreže**

#### **V.**

- 1) Škola ima računalne mreže:
  - bežična mreža Microsoft carnet mreža
  - lokalna mreža – žična mreža u cijelom objektu
- 2) Ciljevi mjera informacijske sigurnosti koje se primjenjuju na školsku računalnu mrežu su: omogućavanje elektroničke komunikacije, neometano korištenje informacija koje su putem računalne mreže dostupne, zaštita školske računalne mreže, zaštita osjetljivih podataka Škole.
- 3) Bežičnu mrežu (WiFi) potrebno je podesiti tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i administrativno osoblje te učenici. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske bežične mreže.
- 4) Ako je potrebno spajati se na školska računala s Interneta, to je potrebno omogućiti isključivo putem sigurnih protokola.
- 5) Nisu svi sadržaji na Internetu primjereni za učenike ili nastavu. Iz tog razloga određeni sadržaji nisu dostupni učenicima kroz školsku mrežu (filtrirani su). Škola može zatražiti od CARNeta reviziju filtriranog sadržaja.

6) Škola zadržava pravo nadzora mrežnog prometa.

## **PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKIM TEHNOLOGIJAMA**

### **Pristup IKT opremi i sigurnost korisnika**

#### **VII.**

- 1) Računala moraju biti podešena tako da traže prijavu korisnika (npr. autentikacijom putem AAI sustava) prije početka rada.
- 2) Preporučuje se korištenje lozinki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 8 znakova.
- 3) Svi računalni programi moraju se koristiti u skladu sa zakonskim propisima i pripadajućim licencama.
- 4) Svi korisnici školskih računala moraju se prijaviti na sustav prije korištenja i odjaviti nakon završetka korištenja. Prijava i odjava korisnika mora uključivati minimalno korištenje korisničkog imena i pripadajuće lozinke, a poželjno i upotrebu certifikata odnosno pametne kartice koji jednoznačno i vjerodostojno identificiraju korisnika
- 5) Učenici na računala ne smiju instalirati nikakve korisničke programe bez dozvole. Ako učenici žele instalirati neke korisničke programe, mogu se obratiti svom učitelju, učitelju informatike ili ravnatelju škole.
- 6) Korisnici su obvezni čuvati podatke i kartice koje koriste za pristup računalima i programima tajnima.
- 7) Korisnici ne smiju koristiti tuđe pristupne podatke za korištenje računala. Ako je to potrebno zbog obavljanja radnih zadaća, nužno je tražiti suglasnost osobe čiji pristupni podaci se koriste. Osoba koja je dala svoje pristupne podatke na korištenje mora što prije promijeniti svoje pristupne podatke.
- 8) Pravila pristupa učenika i zaposlenika škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati.
- 9) Zadnji nastavni dan učenika odnosno radni dan učitelja u školi potrebno je isključiti sva njegova prava pristupa školskim računalima. Nakon isteka ueničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno isključiti
- 10) Učenici smiju koristiti samo školska računala namijenjena njima. Vlastita računala i pametne telefone tijekom nastave učenici smiju koristiti isključivo u obrazovne svrhe uz

prethodnu dozvolu učitelja. Pri tome učenici moraju paziti da ne ugrožavaju druge korisnike Školske mreže širenjem virusa i drugih zlonamjernih programa.

### **Ponašanje na internetu**

#### **VIII.**

- 1) Korisnici su dužni prilikom upotrebe IKT opreme primjenjivati osnovna pravila lijepog ponašanja, ponašati se odgovorno i u skladu s etičkim načelima i u stvarnom i virtualnom svijetu. Prema drugim korisnicima moraju se ponašati pristojno, ne smiju ih vrijeđati ili objavljivati neprimjerene sadržaje.
- 2) Svi korisnici, a posebno učenici, moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na internetu te trebaju biti svjesni publike. (kolege, potencijalni poslodavci, suradnici i sl.) Uvijek moraju imati na umu da i njihova privatna aktivnost u društvenim medijima može utjecati na školske rezultate te da su njihove aktivnosti dostupne za pregled drugim korisnicima.
- 3) Fotografiranje i snimanje osoba smije se napraviti samo uz prethodno dopuštenje. Potrebno je imati dopuštenje za objavu takvih digitalnih sadržaja.
- 4) Korisnici su odgovorni za sve neželjene posljedice upotrebe interneta.
- 5) Korisnici moraju promišljeno dijeliti svoje osobne podatke na internetu te osvijestiti da, kad se jednom pojavi podatak na internetu, više ga nije moguće trajno ukloniti. Prilikom dijeljenja tuđih osobnih podataka korisnici su dužni pridržavati se važećih propisa iz područja zaštite osobnih podataka i tajnosti podataka.
- 6) Učenici trebaju dobro uravnotežiti vrijeme odvojeno za korištenje Interneta, s drugim oblicima nastave, učenja i odmora.
- 7) Korisnici moraju imati na umu da sadržaji koji se nalaze na Internetu ne moraju biti provjereni niti istiniti. Zato sve činjenice koje nađu na Internetu moraju koristiti s oprezom.
- 8) Učenici svakako trebaju koristiti informacije s Interneta u skladu s učiteljevim uputama. Svi sadržaji koji se koriste kao izvor informacija za nastavu moraju se koristiti iz provjerenih izvora.
- 9) 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. Nadalje, zaobilazanje sigurnosnih postavki moglo bi ugroziti održavanje nastave. Ako učenik smatra da je određeni sadržaj neopravdano blokiran ili propušten može se obratiti svom učitelju ili učitelju informatike. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti svog učitelja, učitelja informatike ili ravnatelja.

10) Učenici se moraju pridržavati i drugih uputa koje im mogu dati učitelji, a koje imaju za cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

## **Internetsko nasilje**

### **IX.**

1) Internetsko nasilje općenito se može definirati kao namjerno i opetovano nanošenje štete upotrebom računala, mobitela i drugih elektroničkih uređaja. Nasilje preko interneta, u svijetu poznato kao cyberbullying, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro.

2) Postoje različiti oblici internetskog nasilja:

- Nastavljanja slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem
- Nasilje na chatu, forumu, blogu, društvenim mrežama
- Svi ostali oblici nasilja preko interneta
- Otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima
- Lažno predstavljanje žrtve na internetu
- Slanje uznemirujućih i/ili prijetećih poruka žrtvi koristeći različite internetske servise (Facebook, Skype, e-mail...)
- Postavljanje internetske ankete o žrtvi
- Slanje virusa na e-mail ili mobitel
- Slanje uznemirujućih fotografija putem e-maila, MMS-a ili drugih komunikacijskih alata
- Krađa ili promjena lozinke za e-mail ili nadimka na chatu

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

4) Škola redovito provodi edukaciju o neprihvatljivom ponašanju kroz predmete koji koriste tehnologiju ili sat razrednika, a pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva su u prostorijama škole.

5) 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.

6) Škola se obvezuje da će:

- podučiti učenike i učitelje o mogućim oblicima internetskog nasilja
- učenike i učitelje podučiti o tome kako prepoznati internetsko nasilje.
- jasno istaknuti prihvatljiva pravila ponašanja te o njima podučiti učenike kroz predmete koji koriste tehnologiju.
- razviti nultu stopu tolerancije na internetsko nasilje.
- obilježavati Dane sigurnog korištenja interneta i suzbijanja nasilja kroz kreativne radove (npr. natječaj za najbolji video uradak, likovni ili literarni uradak na temu internetskog nasilja kako se potaknula svijest o temi među učenicima).

## **PRIJELAZNE I ZAVRŠNE ODREDBE**

### **X.**

- 1) Ovaj Pravilnik stupa na snagu danom donošenja i objavljuje se na web stranici škole.

KLASA: 012-02/19-01/01

URBROJ: 251-176-19-1

Zagreb, 29.01.2019.

Ravnatelj:

---

Vatroslav Gabrić, prof