Jožef Stefan
Trst

DRŽAVNI IZOBRAŽEVALNI ZAVOD
S SLOVENSKIM UČNIM JEZIKOM
ISTITUTO STATALE
DI ISTRUZIONE SUPERIORE
CON LINGUA DI INSEGNAMENTO SLOVENA

NOTRANJI PREDPISI ZA VARNO UPORABO DIGITALNIH UČNIH PLATFORM V OBLAKU

Sprejeto na zavodskem svetu dne 30. 5. 203 s sklepom št. 16/2023

Člen 1: Uvod

Namen tega pravilnika je zagotoviti navodila šolskemu osebju za varno uporabo platform digitalnega učnega oblaka Google Workspace for Education. Uporaba platforme v oblaku je bistvenega pomena za zagotavljanje spletne in digitalne učne izkušnje, enako pomembno pa je preprečiti kakršno koli tveganje za varnost osebnih podatkov učencev.

Člen 2: Registracija in dostop

Ob registraciji bo skrbnik platforme v oblaku odprl profil z imenom in priimkom uporabnika, ki mu bo dodeljen institucionalni e-poštni predal. Na platformo ne bodo naloženi nobeni drugi osebni podatki, uporabnik pa naj sam v svoj profil ne dodaja drugih osebnih podatkov, kot so naslov prebivališča, telefonska številka, osebni elektronski naslov ali fotografija. Dostop do aplikacij in storitev platforme bo potekal prek institucionalnega e-poštnega naslova in vnosa ustreznega gesla za dostop. Dostopne podatke ali račun je prepovedano deliti z drugimi osebami, vključno z osebjem šole ali učenci.

Člen 3: Uporaba drugih aplikacij

Zaposleni morajo uporabljati samo platforme v oblaku, ki jih je odobrila šola, uporaba nedovoljenih ali nezanesljivih platform ali aplikacij v oblaku pa je prepovedana. Če učitelji želijo sprejeti nove aplikacije, jih morajo predložiti v odobritev ravnatelju, ki oceni stopnjo njihove varnosti.

Člen 4: Varstvo osebnih podatkov

Zaposleni na šoli so dolžni dosledno spoštovati predpise o zasebnosti in varstvu osebnih podatkov učencev v skladu s pravno podlago za obdelavo, ki je zagotovljena za izvajanje javnih storitev. Zato je prepovedano zbirati, uporabljati ali razkrivati kakršne koli osebne podatke učencev brez upoštevanja zakonodaje in brez nadzora šolskega pooblaščenca za varstvo osebnih podatkov. Pri uporabi platforme mora vsak uporabnik sprejeti načelo minimiziranja osebnih podatkov, tako da ti niso navedeni, razen če je to potrebno. To načelo minimizacije je treba še posebej strogo upoštevati za podatke, ki razkrivajo rasno ali etnično poreklo, verska ali filozofska prepričanja, politična mnenja, članstvo v sindikatu, zdravje ali spolno življenje

(občutljivi podatki). Učitelji morajo ta načela upoštevati tudi pri dodeljevanju dejavnosti in nalog učencem, ki po možnosti ne smejo razkrivati osebnih in zlasti občutljivih podatkov.

Člen 5: Deljenje vsebine

Šolsko osebje je odgovorno za vsebino, ki se deli na platformah v oblaku za podporo poučevanju. Zato naj osebje skrbno preveri pravilnost in točnost vsebine, preden jo začne deliti, in naj ne deli žaljive, diskriminatorne ali nezakonite vsebine. Poleg tega je prepovedano uporabljati platforme v oblaku za deljenje vsebin, zaščitenih z avtorskimi pravicami ali intelektualno lastnino, brez izrecnega dovoljenja lastnika.

Člen 6: Varnost

Šolsko osebje mora uporabljati platforme v oblaku na varen in odgovoren način ter zagotavljati zaščito svojih osebnih podatkov in osebnih podatkov učencev. Uporabljajo se lahko le nujno potrebni podatki za izvajanje načrtovanih dejavnosti. Zato naj osebje ne namešča ali uporablja nepooblaščene ali nevarne programske opreme in naj svoje naprave stalno posodablja z najnovejšimi varnostnimi posodobitvami. Poleg tega je prepovedano dostopati do platform v oblaku iz nezavarovanih javnih omrežij.

Člen 7: Pravilna uporaba virov

Šolsko osebje je dolžno uporabljati platforme v oblaku za podporo poučevanju samo v izobraževalne in učne namene. Uporaba platform v oblaku za osebne ali komercialne dejavnosti ni dovoljena. Poleg tega je prepovedana uporaba platform v oblaku za oglaševanje, politično propagando ali katero koli drugo dejavnost, ki bi se lahko štela za neprimerno ali bi lahko kršila veljavne zakone ali šolske politike.

Člen 8: Shranjevanje podatkov

Vsi podatki, shranjeni na platformah v oblaku, morajo biti ustrezno zaščiteni pred nepooblaščenim dostopom, izgubo ali poškodbo. Osebje mora zato zagotoviti, da so datoteke z osebnimi podatki shranjene v varnih delih platform, dostop do njih pa je omejen le na zaposlene ali pooblaščene učence ali starše. Ta varnostni ukrep je treba še posebej strogo upoštevati v primeru, da se na platformi shranjujejo občutljivi podatki, pri čemer je treba razmisliti tudi o tehnikah psevdonimizacije (glej člen 11).

Poleg tega je potrebno pozorno nadzirati prostor za arhiviranje in redno brisati podatke, ki jih ne potrebujete več, da bi zagotovili varnost in zasebnost podatkov o dijakih. Zlasti ob koncu

šolskega leta je treba izbrisati in po potrebi vrniti vse dokumente in listine, ki so jih učenci izdelali med letom. Pri dokumentih, predloženih v ocenjevanje, upoštevajte okrožnico št. 44 z dne 19. 12. 2005 Generalnega direktorata za arhive - "Arhivi šolskih ustanov", ki predpisuje hrambo najmanj eno leto, hrambo vzorčne dokumentacije pa eno leto na deset let.

Člen 9: Dostop do podatkov

Osebje mora zagotoviti, da je dostop do podatkov o dijakih omejen le na pooblaščene člane osebja, ki te podatke potrebujejo za opravljanje svojega dela. V primeru dvoma se mora osebje obrniti na ravnatelja ali pooblaščenca za varstvo podatkov, da potrdi, da je obdelava določenega sklopa podatkov upravičena.

Člen 10: Varnost gesel

Osebje mora za dostop do platform v oblaku uporabljati močna in zapletena gesla. Gesla morajo biti edinstvena in se ne smejo uporabljati v drugih platformah ali storitvah. Poleg tega je treba gesla redno spreminjati, da se prepreči nepooblaščen dostop.

Člen 11 - uporaba tehnik psevdonimizacije za podatke v skladu s členom 9 SUVP

V tem oddelku "občutljivi podatki" pomenijo kategorije osebnih podatkov iz člena 9 Splošne uredbe o varstvu podatkov (GDPR), tj. podatke, ki razkrivajo rasno ali etnično poreklo, verska ali filozofska prepričanja, politična mnenja, članstvo v sindikatu, zdravje ali spolno življenje. Za te kategorije osebnih podatkov mora šolsko osebje zagotoviti maksimalno varnost in zaupnost v skladu z GDPR in Kodeksom zasebnosti. Osebni podatki občutljive narave se lahko naložijo na platformo v oblaku le, če je to nujno potrebno in če ni izvedljivih alternativnih rešitev. V tem primeru mora šolsko osebje uporabiti tehnike psevdonimizacije z zamenjavo osebnih podatkov, ki identificirajo posameznika, na katerega se nanašajo osebni podatki (na primer ime in priimek), s kodo, ki brez dodatnih informacij ne omogoča identifikacije posameznika. Psevdonimizacijo je treba uporabiti za vse občutljive podatke, vključno s podatki o zdravju učencev in šolskega osebja, če se obdelujejo.

Člen 12: Varnost naprave

Uslužbenci morajo za dostop do platform v oblaku le varne in posodobljene naprave. Osebne naprave se ne smejo uporabljati za dostop do občutljivih podatkov učencev, razen če so ustrezno zaščitene z zanesljivimi gesli in posodobljeno varnostno programsko opremo.

Člen 13: Upravljanje kršitev varstva osebnih podatkov

Zavod je za upravljanje kršitev varstva osebnih podatkov (data breach) pripravil posebne smernice in izdal okrožnico za zaposlene, da bodo lahko prepoznali nastanek kakršne koli kršitve, četudi le potencialne ali domnevne, in posledično ukrepali. Na tem mestu bi radi opozorili na določbe, ki zahtevajo, da sta skrbnik platforme v oblaku oz. ravnatelj obveščena o vsaki kršitvi varstva osebnih podatkov, za katero sta izvedela. Za informacije ali zahteve po pojasnilih se lahko obrnete tudi na pooblaščenca za varstvo podatkov, ki ga imenuje ravnatelj. Osebje mora v celoti sodelovati pri vseh notranjih ali zunanjih preiskavah kršitev podatkov ali kršitev te politike. Kršitve te politike se obravnavajo zelo resno in se lahko končajo z disciplinskimi ukrepi, vključno z odpustitvijo.