

Směrnice o používání informačních a komunikačních technologií, kybernetická bezpečnost školy	
Č.j.:	ZŠŠK/858/2021
Spisový znak:	1.1.1.
Skartační znak:	A5
Vypracoval:	MVDr. Martin Svoboda
Schválil:	MVDr. Martin Svoboda
Pedagogická rada pojednala dne:	20.1.2022
Směrnice nabývá platnosti ode dne:	1.1.2022

Obsah

1.	Úvodní ustanovení	2
1.1.	Předmět úpravy	2
1.2.	Základní pojmy	2
2.	Uživatelé ICT	2
2.1.	Obecné chování uživatelů	2
2.2.	Přístupy do systému a uživatelské účty	3
2.3.	Žáci	4
2.4.	Zaměstnanci	4
2.5.	ICT pracovník	4
3.	Provoz na serverech a nakládání s daty	5
3.1.	Provoz na serverech	5
3.2.	Práce a nakládání s daty	5
3.3.	Evidence osobních údajů v elektronickém systému, dálkový přístup	5
4.	Závěrečná ustanovení	6
4.1.	Porušení pravidel a následné postupy	6

1. Úvodní ustanovení

1.1. Předmět úpravy

- 1) Tato směrnice stanovuje pravidla používání informačních a komunikačních technologií, provozu počítačové sítě, chování jejich uživatelů, nakládání s hardwarem, softwarem a audiovizuální technikou (dále jen ICT) na Základní škola Havířov-Šumbark Školní 1/814 okres Karviná, příspěvková organizace, dále jen škola.
- 2) Tato směrnice je závazná pro všechny uživatele ICT školy.
- 3) Uživatelem ICT ve škole jsou:
 - a) zaměstnanec v pracovně právním poměru, zaměstnanec pracující na základě dohody o provedení práce nebo dohody o pracovní činnosti;
 - b) pracovník na jiný typ smlouvy podle občanského nebo obchodního zákoníku, jehož práce je vykonávána prostřednictvím nebo s využitím ICT;
 - c) žák, student, klient školy;
 - d) další fyzická osoba, již bylo povoleno na základě žádosti či uzavřené smlouvy využití ICT.

1.2. Základní pojmy

POJEM	VÝZNAM
Hardware	Souhrn technických prostředků informační a komunikační techniky. Jde především o počítače a jejich komponenty, periferie (tiskárny, monitory apod.) a prvky datových sítí včetně jejich komponentů.
Heslo	Unikátní řetězec písmen, číslic a znaků pro ověření totožnosti uživatele při přístupu k elektronickým systémům.
ICT	Informační a komunikační technologie.
Klient	Zařízení v počítačové síti, využívající služeb serveru.
Licence	Oprávnění k výkonu práva užívat software stanovené licenční smlouvou nebo licenčním ujednáním.
Licenční smlouva a licenční ujednání	Právní dokument, kterým autor poskytuje nabyvateli oprávnění k výkonu práva užití software stanoveným způsobem a ve stanoveném rozsahu.
Notebook	Přenosný osobní počítač.
Pracovní stanice	Osobní počítač včetně příslušných periférií.
Server	Počítač v počítačové síti, který poskytuje služby klientům.
Software	Programové vybavení hardwarových prostředků.
Uživatelské jméno	Identifikace uživatele počítačového systému – majitele uživatelského účtu.
Wi-Fi	Bezdrátové připojení k síti.

2. Uživatelé ICT

2.1. Obecné chování uživatelů

- 1) Uživatel ICT školy: ten, kdo využívá oprávněně prostředky ICT školy. Musí se chovat tak, aby neporušoval platný právní řád České republiky a ostatní vnitřní směrnice školy.
- 2) Povinnosti uživatele ICT:
 - a) hlásit bez prodlení ICT pracovníkovi jakékoliv podezření na porušení této směrnice, závadné chování jiných uživatelů ICT ve škole (např. zneužití přístupu do sítě, podezření na nelegální činnost, odcizení či zneužití dat), závady hardwaru, podezření na použití nelegálního softwaru, chyby v softwaru či špatné fungování softwaru;

- b) využívat ICT vybavení školy pouze pro vzdělávací účely, doplňkovou činnost nebo úkoly související s provozem a správou školy;
 - c) užívat k práci na pracovní stanici nebo notebooku ve vlastnictví školy pouze legálního softwaru, který je určený k plnění pracovních povinností nebo ke vzdělávání;
 - d) starat se o soukromá zařízení, která jsou připojena do sítě školy, tzn. mít je zabezpečená tak, aby nedocházelo k narušení bezpečnosti a omezování v provozu internetu (intranetu). Vyžaduje se instalace antivirové ochrany, firewallu a jiných bezpečnostních programů.
- 3) Uživatelům ICT je zakázáno:
- a) využívat prostředky ICT k soukromým nebo jiným účelům nesouvisejícím s činností školy;
 - b) vystavovat prostředky ICT jakémukoliv nebezpečí poškození;
 - c) zprostředkovat přístup k prostředkům ICT školy fyzickým či právnickým osobám, které nejsou uživateli ICT školy, kromě osob, které mají na starost instalace a údržbu softwaru;
 - d) poškozovat jakoukoli součást prostředků ICT školy;
 - e) používat prostředky ICT, které nejsou v majetku školy, v počítačové síti školy s výjimkou, přenosných disků nebo pamětí, sluchátek s mikrofonom, fotoaparátů a kamer;
 - f) odstraňovat informace nebo označení identifikující autorská práva k softwaru;
 - g) pracovat pod cizí identitou, používat prostředky k jejímu získání nebo zneužít pro tento záměr pochybení či nedbalosti jiného uživatele;
 - h) sledovat nebo odposlouchávat provoz sítě;
 - i) spouštět nebo instalovat jakýkoliv software (zvláště software zvyšující zatížení sítě) a vyvarovat se další činnosti, která vede k zatížení sítě nebo omezení služeb;
 - j) zapojovat do sítě zařízení, která mohou ovlivnit komunikační provoz sítě (např. přepínače, směrovače aj.);
 - k) na svých zařízeních v síti školy používat serverové aplikace nebo skenovací a penetrační nástroje, zejména síťové doménové řadiče, DHCP servery, licenční servery apod.;
 - l) provádět výměny, stěhování, čištění, odpojení či připojení k datové síti, opravy a změny konfigurace software a hardware bez účasti ICT pracovníka, s výjimkou odpojení a připojení přenosných datových nosičů.

2.2. Přístupy do systému a uživatelské účty

- 1) Účet zaměstnance je zřízen na základě zadání uživatele do systému.
- 2) Každý uživatel ICT si při prvním přihlášení změní heslo. Nová hesla se tvoří podle těchto pravidel:
 - heslo je tvořeno nejméně 10 znaky;
 - heslo musí obsahovat alespoň jedno velké písmeno, číslici a speciální znak;
 - heslo by nemělo obsahovat textové nebo číselné údaje, které lze odvodit ze známých údajů účastníka, např. jméno účastníka, jeho příbuzných, bydliště, SPZ jeho auta, datum narození, rodné číslo, telefonní číslo apod.;
 - heslo k uživatelskému účtu by nemělo být použito pro jiné aplikace (soukromý e-mail, facebook, uživatelské programy aj.);
- 3) Uživatel ICT je povinen udržovat heslo v tajnosti a nezaznamenávat jej způsobem, který umožní dostupnost hesla dalším osobám.
- 4) Pomocí přiděleného uživatelského jména a hesla se přistupuje do elektronických aplikací školy.
- 5) Účet zaměstnance je zrušen po zadání informace o ukončení právního vztahu ke škole do informačního systému školy.
- 6) Žáci se přihlašují žákovskými účty k výukovému software a internetovému vyhledávači.

- 7) Povinností ICT pracovníka je minimálně jednou za rok provádět kontrolu aktivních účtů.

2.3. Žáci

- 1) Žáci užívají hardware a software školy pro účel, ke kterému je určen. Jde zejména o využívání počítačů v počítačových učebnách.
- 2) Před opuštěním pracovní stanice jsou žáci povinni se odhlásit ze všech aplikací a operačního systému.
- 3) Žáci nejsou oprávněni připojovat se s vlastním zařízením do sítě školy.
- 4) Škola může poskytnout žákům a studentům software, který lze podle licenčního ujednání použít pro studenty v rámci jejich samostudia.

2.4. Zaměstnanci

- 1) Základní zásady ochrany dat na pracovních stanicích a notebookech (počítačích), které má ve vlastnictví škola, jsou následující:
 - a) Zaměstnanec je oprávněn využívat k práci pouze počítač, který mu byl k jeho práci přidělen, který je určen pro společné používání ve sborovně a v kabinetech nebo počítače v místnostech určených pro výuku.
 - b) Přístup zaměstnanců na počítač přidělený jinému uživateli je možný pouze se svolením tohoto uživatele, a to vždy pouze pod vlastní identitou. Zaměstnanec smí umožnit přístup na přidělený počítač pouze uživatelům ICT školy.
 - c) Při opuštění pracoviště se každý zaměstnanec odhlásí z aplikací a operačního systému, zamkne nebo vypne pracovní stanici a dále zabezpečí pracoviště před vstupem neoprávněné osoby.
- 2) Všechny pracovní stanice a notebooky zaměstnanců jsou připojeny do internetu prostřednictvím počítačové sítě školy. Vedoucí pracovník může z důvodu bezpečnosti nařídit ICT pracovníkovi odpojení pracovní stanice nebo notebooku.
- 3) V aplikacích, umožňujících přístup k osobním údajům, jsou uživatelé přihlášení jen po nezbytně nutnou dobu, kdy s aplikací skutečně pracují.
- 4) Zakazuje se otevírat přílohy e-mailů se soubory umožňující spustit škodlivý kód (zejména soubory s příponou exe, bat, com, dll, lnk, msi, reg, 386, bin, chm, cmd, vbs aj.).

2.5. ICT pracovník

- 1) ICT pracovník je oprávněn k přístupu ke všem pracovním stanicím a notebookům ve vlastnictví školy a k datům na nich uloženým. Musí přitom dbát, aby jeho činnost byla v souladu s obecným nařízením GDPR a českým adaptačním zákonem ke zpracování osobních údajů.
- 2) ICT pracovník zajišťuje celkovou správu ICT v počítačové síti školy. Provoz sítě, aplikací a přístupů k nim.
- 3) Povinnosti ICT pracovníka:
 - a) Chrání zabezpečení ICT školy.
 - b) Chrání uživatelské a administrátorské přístupové údaje na servery, datová úložiště a do aplikací.
 - c) Poskytuje uživatelskou podporu, konzultace a pomoc uživatelům.
 - d) Nesdílí přístupové informace na zařízení a aplikace školy třetím osobám, dodavatelům i dalším zaměstnancům, kteří nemají provoz daného serveru nebo aplikace v kompetenci.

- e) Stará se o údržbu a kontrolu softwaru a hardwaru pracovních stanic, notebooků a o jejich antivirovou ochranu, má plný přístup k určeným zařízením a musí mu být umožněn přístup k hardwaru a softwaru.
- f) Zajišťuje instalace softwaru na pracovní stanice v objektu školy.

3. Provoz na serverech a nakládání s daty

3.1. Provoz na serverech

- 1) Každý zaměstnanec školy má přiděleno diskové úložiště na logickém oddílu disku označeném velkým písmenem a dvojtečkou (např. Z:) nebo na lokálním disku pracovní stanice.
- 2) Přístup do dalších umístění souborového serveru je dán pracovním nebo studijním zařízením.
- 3) Za obsah diskového úložiště ručí vždy majitel účtu, za obsah na sdíleném diskovém úložišti ručí jeho vlastník. Na diskové úložiště nesmí být ukládány soubory nesouvisející s výukou nebo s výkonem práce. Z obsahu mohou být vymazány nebezpečné typy souborů a soubory audio a video. Uživatel je o smazání obsahu informován.
- 4) Škola vymaže obsah složek cílových úložišť u žáků vždy po ukončení PŠD, nebo odchodu žáka ze školy.

3.2. Práce a nakládání s daty

- 1) Uživatelé jsou povinni při nakládání s daty, tzn. při jejich pořizování, zpracovávání, archivaci a šíření, dodržovat obecně závazné právní předpisy České republiky a vnitřní předpisy.
- 2) Uživatel je povinen zajistit ochranu dat před zneužitím a ztrátou. Škola neodpovídá za ztrátu a zneužití dat způsobené nedbalostí či chybou uživatele.
- 3) Pořizování databází, datových sad či jiných celistvých datových struktur, které nejsou volně šiřitelné, a nakládání s nimi musí být vždy podloženo smluvním ujednáním s poskytovatelem těchto dat. Smluvní ujednání musí obsahovat zejména podmínky a způsob, jak může škola oprávněně s daty nakládat, včetně možnosti a rozsahu jejich dalšího šíření. Nestanoví-li obecně závazné právní předpisy jinak, musí být tyto podmínky sjednány v písemné smlouvě.
- 4) Není-li si uživatel jist jakýmkoliv aspektem pořizování, zpracovávání, archivaci a šíření dat, je povinen konzultovat problematiku s nadřízeným pracovníkem nebo ICT pracovníkem a v případě, že se jedná o osobní údaje, může škola problém konzultovat a řešit s pověřencem na ochranu osobních údajů.

3.3. Evidence osobních údajů v elektronickém systému, dálkový přístup

- 1) Škola eviduje osobní údaje zaměstnanců a žáků v elektronickém systému Bakaláři.
- 2) Pedagogičtí pracovníci mají v omezené míře přístup k osobním údajům žáků pro zapisování osobních údajů a zadávání klasifikace.
- 3) Zaměstnanci, kteří mají dálkový přístup k osobním údajům, jsou povinni přistupovat k nim pouze tehdy a tak, aby k osobním údajům nemohla přistupovat neoprávněná osoba. Dálkový přístup neprovádějí na veřejných místech a na veřejných počítačích (knihovna, internetová kavárna apod.).
- 4) V případě, že dálkový přístup provádějí prostřednictvím svého vlastního mobilního zařízení nebo zařízení určeného školou - zařízení (mobilní telefon, tablet, notebook), musí toto zařízení zabezpečit pro případ ztráty nebo krádeže. To znamená, že zařízení je zabezpečeno heslem, PINem, otiskem prstu apod. a že v něm nebudou uložena v jakékoliv podobě přístupová hesla do aplikací umožňujících dálkový přístup k osobním údajům.

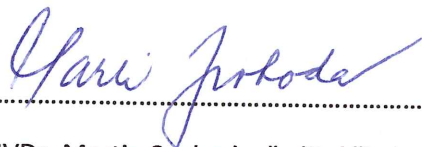
- 5) Zákonní zástupci žáků školy mají v omezené míře přístup k osobním údajům žáků, týkajících se docházky, prospěchu a chování.

4. Závěrečná ustanovení

4.1. Porušení pravidel a následné postupy

- 1) Při porušení pravidel stanovených touto směrnicí, případně dalšími obecně závaznými právními předpisy v oblasti ICT, se postupuje vždy vzhledem k závažnosti tohoto porušení.
- 2) Při jakémkoliv zjištění porušení pravidel se nejprve zajistí náprava tak, aby nedošlo ke škodě na zdraví, majetku, či nedošlo k přestupku nebo trestnému činu. Pokud již došlo ke škodě či přestupku nebo trestnému činu, je povinností všech zúčastněných stran co nejvíce minimalizovat škody či dopad na provoz školy.
- 3) Povinností uživatele ICT je hlásit ICT pracovníkovi jakékoliv porušení či podezření na porušení pravidel (podkapitola 2.1, odstavec 2 a) této směrnice). Povinností ICT pracovníka je problémovou situaci neprodleně řešit s:
 - a) bezprostředně nadřízeným zaměstnancem, týká-li se porušení či podezření na porušení pravidel zaměstnancem v pracovním poměru nebo pracovníkem na dohodu o provedení práce či na dohodu o pracovní činnosti;
 - b) třídním učitelem, výchovným poradcem, týká-li se porušení či podezření na porušení pravidel žákem školy.

V Havířově 31.12.2021



MVDr. Martin Svoboda, ředitel školy

ZÁKLADNÍ ŠKOLA
Havířov - Šumbark ©
Školní 1/814, okres Karviná
příspěvková organizace
IČO:70958149 tel:596 684 808