|  |  |
| --- | --- |
| SMĚRNICE O POUŽÍVÁNÍ INFORMAČNÍCH A KOMUNIKAČNÍCH  TECHNOLOGIÍ („ICT směrnice“) | |
| Vypracoval/a: | Jakub Jeník, správce sítě |
| Schválil/a: | Mgr. Jana Hurdová, ředitelka školy |
| Pedagogická rada projednala dne | 28.08.2025 |
| Směrnice nabývá platnosti dne | 1.9.2025 |
| Změny ve směrnici jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu | |

# Úvodní ustanovení

## 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 škole v Novosedlicích** (dále jen *škola*).
2. Tato směrnice je závazná pro všechny uživatele ICT školy.
3. Uživatelem ICT ve škole jsou:
   1. zaměstnanec v pracovně právním poměru, zaměstnanec pracující na základě dohody o provedení práce nebo dohody o pracovní činnosti;
   2. pracovník na jiný typ smlouvy podle občanského nebo obchodního zákoníku, jehož práce je vykonávána prostřednictvím nebo s využitím ICT;
   3. žák školy;
   4. další fyzická osoba, jíž bylo povoleno využití ICT na základě žádosti či uzavřené smlouvy.

## Základní pojmy

|  |  |  |
| --- | --- | --- |
| **Č.** | **POJEM** | **VÝZNAM** |
| 1 | DHCP | Protokol pro automatické přidělování IP adres jednotlivým síťovým zařízením v počítačových sítích. |
| 2 | DoS, DDoS | Typ útoku na přetížení služeb a serverů. Útok cílovou službu znefunkční a znepřístupní ostatním uživatelům. |
| 3 | 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. |
| 4 | Heslo | Unikátní řetězec písmen, číslic a znaků pro ověření totožnosti uživatele při přístupu k elektronickým systémům. |
| 5 | ICT | Informační a komunikační technologie. |
| 6 | Internetová doména | Unikátní adresa na internetu, tzv. doménové jméno. |
| 7 | Internet | Veřejná počítačová síť. |
| 8 | Intranet | Privátní počítačová síť, která je izolovaná od dalších vnějších sítí. |
| 9 | IP adresa | Jednoznačná identifikace zařízení v počítačové síti. |
| 10 | Klient | Zařízení v počítačové síti, využívající služeb serveru. |
| 11 | Licence | Oprávnění k výkonu práva užívat software stanovené licenční smlouvou nebo licenčním ujednáním. |
| 12 | Licenční smlouva a licenční ujednání | Právní dokument, kterým autor poskytuje nabyvateli oprávnění k výkonu práva užít software stanoveným způsobem a ve stanoveném rozsahu. |
| 13 | MAC adresa | Jednoznačný identifikátor síťového zařízení (tzv. fyzická adresa). |
| 14 | Notebook | Přenosný osobní počítač. |
| 15 | P2P | Výměnné sítě, kde spolu komunikují klienti této sítě přímo. |
| 16 | Pracovní stanice | Osobní počítač včetně příslušných periferií. |
| 17 | Režim absolventa | Stav úložiště dat, kdy jsou absolventům vymazána data z jejich diskových úložišť, jsou jim odebrána přístupová práva do všech dříve zpřístupněných systémů a stejně tak i jejich zákonným zástupcům. |
| 18 | Server | Počítač v počítačové sítí, který poskytuje služby klientům. |
| 19 | Software | Programové vybavení hardwarových prostředků. |
| 20 | Uživatelské jméno | Identifikace uživatele počítačového systému – majitele uživatelského účtu. |
| 21 | Wi-Fi | Bezdrátové připojení k síti. |

# Uživatelé ICT

## Obecné chování uživatelů

1. **Uživatel ICT školy** je 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**:
   1. 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;
   2. využívat ICT vybavení školy pouze pro vzdělávací a umělecké účely, doplňkovou činnost nebo úkoly související s provozem a správou školy;
   3. užívat k práci na pracovní stanici nebo notebooku ve vlastnictví školy pouze legálního softwaru, který je určený k plnění pracovních povinností nebo ke vzdělávání;
   4. 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 či intranetu.
3. **Uživatelům ICT je zakázáno**:
   1. využívat prostředky ICT k soukromým nebo jiným účelům nesouvisejícím s činností školy;
   2. vystavovat prostředky ICT jakémukoliv nebezpečí poškození;
   3. 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 nebo mají přístup k datům[[1]](#footnote-1);
   4. poškozovat jakoukoli součást prostředků ICT školy;
   5. používat prostředky ICT, které nejsou v majetku školy, v počítačové síti školy s výjimkou zařízení připojených přes k tomu určenou Wi-Fi síť, povolených přenosných disků nebo pamětí, sluchátek s mikrofonem, fotoaparátů a kamer;
   6. odstraňovat informace nebo označení identifikující autorská práva k softwaru;
   7. pracovat pod cizí identitou, používat prostředky k jejímu získání nebo zneužít pro tento záměr pochybení či nedbalosti jiného uživatele;
   8. sledovat nebo odposlouchávat provoz sítě;
   9. spouštět nebo instalovat jakýkoliv software (zvláště software zvyšující zatížení sítě) a vyvarovat se další činnosti, která vede k zatížení sítě nebo omezení služeb – jedná se především o používání výměnných sítí P2P, DDoS či DoS útoky a/nebo další softwarové nástroje;
   10. zapojovat do sítě zařízení, která mohou ovlivnit komunikační provoz sítě (např. přepínače, směrovače aj.);
   11. na svých zařízeních v síti školy používat serverové aplikace nebo skenovací a penetrační nástroje, zejména služby doménového řadiče, DHCP servery, licenční servery apod.;
   12. 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. Stěhování v rámci školy, jehož součástí je stěhování hardwaru, musí být předem konzultováno s ICT pracovníkem a musí být definovány změny, které nastanou (potřeba změn v konfiguraci počítačové sítě aj.).

## Přístupy do informačních systémů a uživatelské účty

1. Účet uživatele ICT je zřízen do centrálního systému uživatelských účtů na serveru a do jednotlivých informačních systémů na základě požadavku, a to nejpozději do pěti dnů.
2. Uživatel ICT je oprávněn používat pouze přidělené uživatelské jméno a heslo. Uživatelské jméno je vždy unikátní a neměnné. Počáteční heslo je generováno a uživatel jeho převzetí potvrdí podpisem. Uživatel je povinen udržovat heslo v tajnosti a neznamenávat jej způsobem, který umožní dostupnost hesla dalším osobám.
3. Uživatel ICT nesmí předávat své přístupové údaje žádným jiným uživatelům ICT ani jiným osobám. Výjimkou je předání přístupů pracovníku ICT v případě, kdy to vyžaduje řešení konkrétního servisního požadavku.
4. Pomocí přiděleného uživatelského jména a hesla je uživatel oprávněn přistupovat do informačních systémů školy.
5. Každý uživatel ICT si může kdykoliv změnit heslo. Nová hesla se tvoří podle těchto pravidel:
   * heslo **je** tvořeno **nejméně 8 znaky**;
   * heslo **musí** obsahovat alespoň jedno velké písmeno a číslici nebo 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.);
   * heslo změněné uživatelem by nemělo být zaznamenáno písemně ani v nezabezpečeném datovém souboru.
   * heslo **neobsahuje** diakritiku.
6. Pokud je heslo třikrát po sobě zadáno chybně, je automaticky zablokován uživatelský účet. O jeho zpřístupnění s novým heslem musí uživatel požádat ICT pracovníka.
7. Účet zaměstnance je zrušen po ukončení právního vztahu ke škole, a to nejdéle do tří dnů. Účet žáka je převeden do režimu absolvent po ukončení vzdělávání ve lhůtě 1 týdne. Účty dalších fyzických osob jsou zrušeny ihned po skončení období, na které byly zřízeny. Povinností ICT pracovníka je minimálně jednou za rok provádět kontrolu aktivních účtů.

## Žáci

1. Žáci užívají hardware a software školy pro účel, ke kterému je určen. Jde zejména o využívání počítačů, zařízení a aplikací pro studium a samostudium. Dále se jedná o kopírovací a tiskové služby a Wi-Fi připojení.
2. Před opuštěním pracovní stanice jsou žáci povinni se odhlásit ze všech aplikací a operačního systému.
3. Žáci a studenti nejsou oprávněni připojovat se s vlastním zařízením do sítě školy jinak než přes Wi-Fi.
4. Žáci a studenti jsou povinni pro přidělení IP adresy u vlastního zařízení použít protokolu DHCP. Nastavení statické adresy zařízení, brány, či DNS serveru je zakázáno.
5. Odpovědnost za svá soukromá zařízení nesou žáci. Odpovídají především za zabezpečení svých mobilních zařízení (notebooky, tablety, mobilní telefony aj.), antivirovou ochranou a používaným softwarem. V případě zjištění problému s těmito zařízeními je ICT pracovník oprávněn zařízení odpojit a informovat žáka o důvodu odpojení. Po odstranění problému je možné přístup opět povolit.
6. Škola může poskytnout žákům software, který lze podle licenčního ujednání použít pro studenty v rámci jejich samostudia.
7. Třídní učitel je povinen seznámit žáky se závaznými pravidly uvedenými v tomto bodu směrnice a zajistit evidenci o jejich seznámení.

## Zaměstnanci

1. Základní zásady ochrany dat na pracovních stanicích a noteboocích (dále *počítač*), které má ve vlastnictví škola, jsou následující:
   1. Zaměstnanec je oprávněn využívat k práci pouze počítač, který mu byl k jeho práci přidělen, který je určen pro společné používání ve sborovně, v kabinetech, na chodbách školy nebo počítače v místnostech určených pro výuku.
   2. 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.
   3. 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.
   4. Šifrování školních dat a disků zaměstnancem není povoleno. Výjimkou je pouze šifrování prováděné ve spolupráci s ICT pracovníkem v případě, že je nezbytné k ochraně osobních údajů.
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. Pokud práce se softwarovou aplikací vyžaduje přihlášení, smí být zaměstnanec přihlášen jen po nezbytně nutnou dobu, kdy s aplikací skutečně pracuje.
4. V aplikacích, umožňujících přístup k osobním údajům, jsou uživatelé po 10 minutách nečinnosti automaticky odhlášeni.
5. 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.).

## ICT pracovník

1. ICT pracovník je oprávněn k přístupu ke všem ICT prostředkům ve vlastnictví školy a k datům na nich uloženým. Musí přitom dbát, aby jeho činnost byla v souladu s obecným nařízením GDPR[[2]](#footnote-2) 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 je monitorován.
3. Povinnosti ICT pracovníka:
   1. Chrání zabezpečení ICT školy.
   2. Chrání uživatelské a administrátorské přístupové údaje na servery, datová úložiště a do aplikací.
   3. Poskytuje uživatelskou podporu, konzultace a pomoc uživatelům.
   4. Nesděluje přístupové informace na zařízení a aplikace školy třetím osobám, dodavatelům i dalším zaměstnancům, kteří nemají provoz daného serveru nebo aplikace v kompetenci.
   5. 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.
   6. Stará se o zajištění infrastruktury a telekomunikace školy. Kontroluje funkčnost sítě, připojení k internetu a sleduje provoz sítě.
   7. Zajišťuje instalace definovaného softwaru3 na pracovní stanice v majetku školy.

# Provoz na serverech, cloudových službách a nakládání s daty

## Provoz na serverech a cloudové služby

1. **Cloudové komunikační služby**:
   1. Každý uživatel ICT má přidělen školní cloudový účet pro e-mailovou a další komunikaci.
   2. Přesměrování e-mailů mimo doménu školy není povoleno.
   3. Velikost přílohy e-mailu je omezena na 25 MB.
   4. Není dovoleno přijímat nebo odesílat přílohy se soubory umožňující spustit škodlivý kód (zejména soubory s příponou exe, bat, com, dll, lnk, msi, reg, 386, bin, chm, cmd, vbs aj.).
   5. Složka Nevyžádaná pošta je automaticky vymazána po 30 dnech.
   6. Složka Koš je automaticky vymazána po 30 dnech.
2. **Cloudové úložiště, souborové servery a lokální úložiště**:
   1. Každý uživatel ICT má k dispozici osobní cloudové diskové úložiště.
   2. ***Uživatelům ICT je zakázáno ukládat soubory na lokální úložiště počítačů.***
   3. Přístup do dalších umístění cloudového úložiště či souborového serveru je dán pracovním nebo studijním zařazením.
   4. Za obsah osobního diskového úložiště ručí vždy majitel účtu, za obsah na sdíleném diskovém uložišti ručí jeho vlastník. Diskové úložiště je primárně určeno pro soubory související 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. V případě opodstatněné žádosti o obnovu dat je možné okamžitě obnovit data ne starší, než 10 dnů nebo obnovit soubory ze starších záloh, pokud jsou k dispozici.
   5. ICT pracovník ručí za konfiguraci, bezpečnost cloudového úložiště a úložištích na serveru.

## 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 školy.
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 obecné 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.

## Evidence osobních údajů v elektronickém systému, dálkový přístup

1. Škola eviduje osobní údaje zaměstnanců a přístupy k nim v informačním systému uvedeném v příloze č. 3.
2. Škola eviduje osobní údaje dětí, žáků a přístupy k nim v informačním systému uvedeném v příloze č. 3.
3. Pedagogičtí pracovníci mají v omezené míře přístup k osobním údajům žáků pro zapisování údajů do elektronické třídní knihy a zadávání klasifikace.
4. 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.).
5. V případě, že dálkový přístup provádějí prostřednictvím svého vlastního mobilního zařízení nebo zařízení určeného školou, 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.
6. Zákonní zástupci žáků mají v omezené míře přístup k osobním údajům žáků, resp. svých týkajících se docházky, prospěchu a chování. Zákonní zástupci žáků a žáci nemohou prostřednictvím dálkového přístupu zadávat změny v zpřístupněných osobních údajích.

# Závěrečná ustanovení

## 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:
   1. 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;
   2. třídním učitelem, vedoucím vychovatelem, pedagogem volného času, týká-li se porušení či podezření na porušení pravidel žákem školy.

## Platnost, účinnost, zpracování a zveřejnění směrnice

1. Směrnice nabývá platnosti dne 27.08.2025 a účinnosti dne 01.09.2025
2. Směrnici zpracoval a za její aktualizaci odpovídá Jakub Jeník, správce IT.
3. Směrnice bude zveřejněna na všech pracovištích školy a na intranetu školy.

V Novosedlicích dne 27.08.2025

Mgr. Jana Hurdová  
ředitelka organizace

Příloha č. 1

# Uživatelská podpora, řešení havárií a komunikace v ICT

**Uživatelská podpora**

je v oblasti ICT prováděna ICT pracovníkem. Pracovník zajišťuje pro zaměstnance řešení:

1. žádostí o přípravu audiovizuální a ICT techniky do výuky;
2. problémů s počítačem;
3. žádostí o změnu, výměnu telefonního čísla;
4. základní uživatelské podpory pro informační systémy;
5. funkčnosti audiovizuální nebo ICT techniky v učebně;
6. problémů s přihlášením na uživatelský či cloudový účet;
7. softwarových problémů.

V době výuky nebo při práci na počítači zajišťuje uživatelskou podporu pro žáky vyučující nebo dozorující pedagog, případně ve spolupráci s ICT pracovníkem.

**Havárie ICT**

Havárie je mimořádná situace ohrožující chod síťové infrastruktury, školy nebo důležitých ICT služeb. Informace o havárii a případné nedostupnosti služeb zasílá zaměstnancům ICT pracovník. U havárie je nutné dbát na obecné zásady a minimalizaci škod a to především s ohledem na:

1. ochranu zdraví a života;
2. ochranu osobních údajů;
3. ochranu majetku;
4. ochranu ostatních dat.

**Odstranění havárie**

Na odstranění havárie pracuje vždy ICT pracovník. Zprovoznění důležitých a klíčových služeb se děje v pořadí důležitosti:

1. chod sítě;
2. vnitřní doménový systém;
3. souborové servery;
4. telefony;
5. připojení do sítě internet;
6. cloudové služby;
7. informační systémy;
8. další služby.

**Havárie služeb zajišťovaných školou**

1. Zaměstnanec školy musí po zjištění havárie kontaktovat ICT pracovníka nebo svého nadřízeného, který následně kontaktuje ICT pracovníka.
2. ICT pracovník nahlásí havárii a její závažnost vedoucím pracovníkům a dalším zaměstnancům, kterých se závada týká (např. klimatizace, výpadek proudu, požár atd.).
3. Opravu provádí nebo zajistí pracovník, který má provádění oprav v pracovních povinnostech, nikoliv pracovník, který havárii zjistil.
4. V případě závažné havárie je oprávněn všechny systémy, které s havárií souvisí, odpojit ICT pracovník.

**Havárie služeb externích subjektů**

1. Telefonní pevné linky:
   1. ICT pracovník kontaktuje dodavatele a nahlásí poruchu operátorovi.
   2. ICT pracovník spolupracuje s dodavatelem na odstranění závady.
2. Přístup k internetu:

ICT pracovník kontaktuje operátora.

1. Nefunkčnost externích informačních služeb ICT pracovník kontaktuje dodavatele služeb.

Příloha č. 2

# Informační systémy používané ve škole

|  |  |  |  |
| --- | --- | --- | --- |
| **Název softwaru** | **Přístup s heslem** | **Osobní údaje v softwaru** | **Instalace a údržba softwaru** |
| VEMA | ANO | ANO | ICT pracovník, EXT C.A.C spol.s r.o. |
| BAKALÁŘI | ANO | ANO | ICT pracovník |
| AVYS | ANO | ANO | ICT pracovník, EXT L. Bučil |
| CIBUS | NE | NE |  |
| INTRANET ZS | ANO | ANO | ICT pracovník, EXT QuickTech s.r.o. |

Příloha č. 3

# Software používaný k evidenci osobních údajů zaměstnanců:

* SW BAKALÁŘI
* IS VEMA
* Lokální databáze pro webové aplikace

Obsah

[1 Úvodní ustanovení 1](#_Toc129616058)

[1.1 Předmět úpravy 1](#_Toc129616059)

[1.2 Základní pojmy 1](#_Toc129616060)

[2 Uživatelé ICT 2](#_Toc129616061)

[2.1 Obecné chování uživatelů 2](#_Toc129616062)

[2.2 Přístupy do informačních systémů a uživatelské účty 3](#_Toc129616063)

[2.3 Žáci 4](#_Toc129616064)

[2.4 Zaměstnanci 4](#_Toc129616065)

[2.5 ICT pracovník 5](#_Toc129616066)

[3 Provoz na serverech, cloudových službách a nakládání s daty 5](#_Toc129616067)

[3.1 Provoz na serverech a cloudové služby 5](#_Toc129616068)

[3.2 Práce a nakládání s daty 6](#_Toc129616069)

[3.3 Evidence osobních údajů v elektronickém systému, dálkový přístup 6](#_Toc129616070)

[4 Závěrečná ustanovení 7](#_Toc129616071)

[4.1 Porušení pravidel a následné postupy 7](#_Toc129616072)

[4.2 Platnost, účinnost, zpracování a zveřejnění směrnice 7](#_Toc129616073)

[Uživatelská podpora, řešení havárií a komunikace v ICT 8](#_Toc129616074)

[Informační systémy používané ve škole 10](#_Toc129616075)

[Software používaný k evidenci osobních údajů zaměstnanců: XXX 11](#_Toc129616076)

1. Příloha č. 2 [↑](#footnote-ref-1)
2. Nařízení Evropského PARLAMENTU A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů 3 Definováno v příloze č. 2 [↑](#footnote-ref-2)