GDPR v IT

Zpracovala:
VOŠZ a SŠZ, Palachova 35, Ústí nad Labem

Účel, rozsah, uživatelé
Účelem tohoto dokumentu je definovat pravidla pro používání informačního systému a dalších informačních prostředků VOŠZ a SŠZ, Palachova 35, Ústí nad Labem (dále jen "Organizace"). Tato pravidla zahrnují i požadavky 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen GDPR.

Uživateli tohoto dokumentu jsou všichni zaměstnanci.

Definice pojmů
Informační systém je sada programů a dalších podsystémů integrovaných do jednoho celku. V širším pohledu jde o komplex technických prostředků tvořený hardwarem a softwarem, které umožňují vytváření, úpravu, odesílání a sdílení dat. V základní rovině je definován servery a klientskými stanicemi, dále pak síťovou infrastrukturou a dalšími komponenty. Jeho zabezpečení je prioritním úkolem při správě a ochraně osobních dat uživatelů.

Členění dle kompetencí
Správce IT - **Ing. Bc. Jiří Štursa**, tel.: 778 706 273, e-mail: jiri.stursa@szsvzs.cz
odpovídá za správu a provoz informačního systému. Provádí kontrolu, nastavení a další změny, které souvisejí se zájmy a potřebami Organizace a požadavky uživatelů.

Správce aplikace – **Ing. Bc. Jiří Štursa**, tel.: 778 706 273, e-mail: jiri.stursa@szsvzs.cz

Pověřenec GDPR – **Mgr. Libor Prexler**, tel.: 778 706 267, e-mail: libor.prexler@szsvzs.cz
poradní funkce v oblasti ochrany osobních údajů

ENLOGIT – externí správce IT. Odpovídá za správu a provoz serverů. Provádí kontrolu, nastavení a další změny, které souvisejí se zájmy a potřebami Organizace a požadavky uživatelů.

Uživatel - definuje jej každý zaměstnanec Organizace a další osoby, které se podílejí na její činnosti v rámci plnění svých pracovních povinností.

Klasifikace informací
Všechny informace jsou rozděleny do skupin podle úrovně své důvěrnosti. V každé úrovni jsou pak stanoveny povinnosti, které mají uživatelé respektovat a plnit.

Úrovně důvěrnosti	Klasifikační kritéria	Omezení přístupu	Bezpečnostní opatření
Veřejné	Zpřístupnění informací veřejnosti nemůže v žádném případě poškodit organizaci. Jde o informace na	Informace jsou k dispozici veřejnosti.	K zajištění celistvosti informací je využíváno automatické zálohování, které umožňuje obnovu

	webových stránkách, vývěsních deskách, nástěnkách, propagačních materiálech atd.		dat v případě jejich ztráty.
Interní použití	Neoprávněný přístup k informacím může organizaci způsobit menší škody nebo potíže. Jedná se především o interní předpisy, rozhodnutí apod.	Informace jsou k dispozici všem zaměstnancům a pověřeným třetím stranám.	Proškolení uživatelů ohledně nakládání s těmito informacemi, antivirové nástroje, omezení přístupu pouze pověřeným osobám, automatické zálohování dat.
S omezeným přístupem	Neoprávněný přístup k informacím může značně poškodit organizaci. Jedná se např. o osobní údaje.	Informace jsou dostupné pouze konkrétní skupině pověřených zaměstnanců a oprávněným uživatelům třetích stran.	Platí opatření pro správu informací v rámci jejich interního použití. Tyto informace jsou při přenosu šifrovány. Nesmějí být ukládány na jiná než výslovně schválená zařízení.

Ochrana elektronických dat - členění dle kompetencí

Správce IT - plná práva
Pověřenec GDPR – plná práva
Třídní učitel - zápis do matriky a třídní knihy, zápis klasifikace
Učitel - zápis do třídní knihy, zápis klasifikace
Zástupci ředitele - evidence docházky, program Bakaláři
Pověřený pracovník - evidence zaměstnanců, evidence úrazů, správa inventáře
Vychovatel – zápis do denního záznamu, vedení osobních spisů žáků a studentů
Knihovník - evidence knihovny
Zákonný zástupce - přístup ke studijním informacím žáka
Rodiče, žák - přístup ke studijním informacím žáka
Výchovný poradce, školní metodik PP, poradce - přístup k vybraným informacím žáka
Sekretariát – program Bakaláři, matrika, spisová služba, kamerový systém, docházkový systém
Studijní oddělení – program Bakaláři, matrika, spisová služba
Zubní ordinace, odborní vyučující DDH – program Stomatolog
Ekonomické oddělení – programy Fenix, WEMA, CODEXIS, WIN zápočet, spisová služba
Školník, demonstrátor – kamerový systém

Klasifikace školní sítě z hlediska ochrany osobních údajů

Přístup do školní sítě je chráněn pomocí uživatelských účtů a hesel. Síťové služby (DHCP, DNS) jsou obstarávány firewallem, který monitoruje provoz na síti. Připojení k internetu zajišťuje ISP Metropolnet, k jejichž síti je škola připojena optickým kabelem. WiFi síť na škole je řešena na platformě MikroTik.

Škola využívá 3 Windows servery:

Pro aplikaci Bakaláři
Programy ekonomického oddělení
Terminal server pro přístup k aplikaci Bakaláři ze vzdálených lokalit

Tyto 3 servery jsou virtualizované. Zálohy všech serverů jsou ukládány na NAS server, který je dále zálohován na další NAS server, který se nachází v jiné části školy, než ostatní servery. Na všechny servery má administrátorský přístup pouze administrator (společnost Enlogit s.r.o.). Jako kolaborační nástroj (email, kalendář, kontakty, sdílené soubory) škola využívá G Suite od společnosti Google.

Nakládání a zabezpečení školní IT techniky

Zajištění ochrany osobních údajů
Pro zajištění ochrany osobních údajů jsou stanovena následující pravidla:

- správa systémů
- údržba systémů
- ochrana a zabezpečení koncových uživatelských stanic
- ochrana a zabezpečení informačních systémů, dat a aplikací

Pravidla pro užívání IT
Pro uživatele jsou stanovena následující pravidla:

- IT technika se užívá dle zásad osobní odpovědnosti
- odhlásit se z PC před odchodem z pracoviště nebo jej zamknout (Win + L), a to i při přerušení práce, pokud PC zůstane na pracovišti neuzamčeném nebo s přístupem více osob
- po skončení práce vždy vypnout PC
- PC a další koncová zařízení se užívají pouze pro výkon pracovních povinností určených zaměstnavatelem
- zaměstnanci užívají pouze takové systémy a aplikace, které jsou licencované v rámci školy a instalované správcem IT
- správci IT jsou hlášeny nalezené závady, zjištěné chyby a nestandartní chování používaného zařízení
- správci IT jsou hlášeny žádosti o údržbu, opravy a aktualizaci počítačových systémů
- uživatelé provádějí pravidelnou zálohu svých dat
- při práci se služebními notebooky mimo prostory Organizace jsou zaměstnanci povinni užívat, v případě odesílání dat s obsahem vyžadujících šifrování, vhodné šifrovací nástroje

- před každým použitím externího média (zejména USB), je toto médium prověřeno antivirovým nástrojem
- při práci v cloudovém prostředí (emailová komunikace, nahrávání a sdílení dat) zaměstnanci dodržují, že k osobním údajům budou mít přístup pouze oprávněné osoby
- Při odesílání emailů s obsahem vyžadujícím šifrování, jsou uživatelé povinni použít vhodné šifrovací nástroje
- všechny počítače zaměstnanců jsou zaheslované správcem IT, jednotliví uživatelé jsou v souvislosti s ochranou svého hesla povinováni mlčenlivostí
- není-li uživatel na svém pracovišti, musí být veškeré papírové dokumenty a média pro ukládání dat, které jsou označeny jako citlivé, odstraněny z pracovního stolu nebo jiných míst (tiskárny, kopírky, skenery apod.), aby se zabránilo neoprávněnému přístupu k nim.

Uživatelům je zakázáno:
- přenášet koncové zařízení bez souhlasu správce IT
- zasahovat do operačního systému a instalovaných aplikací
- měnit systémovou konfiguraci a strukturu adresářů OS
- instalovat či odinstalovávat jakékoliv školní aplikace, včetně volně šiřitelných z internetu
- dále šířit jakékoliv školní aplikace, včetně licenčních kódů a HW klíče
- provádět nezodpovědnou nebo dokonce zlomyslnou činnost na internetu (rozesílání spamů, šíření virů, přetěžování sítí masívním nebo trvalým downloadem či uploadem nebo generováním útoků na webové služby či databáze
- data a informace s klasifikací “s omezeným přístupem” a další citlivé osobní informace ukládat na jiných zařízeních, než na zařízením určených organizací
- data a informace s klasifikací “s omezeným přístupem” a další citlivé osobní informace vynášet mimo organizaci
- pro práci s daty a informacemi s klasifikací “s omezeným přístupem” a dalšími citlivými osobními informacemi používat přenosná externí média (např. USB).

Ochrana osobních údajů:
- uživatelé jsou povinni zachovávat mlčenlivost o informacích obsažených v souborech, databázích či informačních systémech a o všech dalších skutečnostech, o nichž se dozvědí v souvislosti s výkonem práce v rámci svého pracovního poměru ve škole
- o těchto skutečnostech jsou povinni zachovávat mlčenlivost i po skončení pracovního poměru ve škole
- skutečnosti chráněné školským zákonem (§ 28) a osobní údaje lze zpracovávat jen se souhlasem zaměstnavatele a za účelem, který zaměstnavatel stanoví
- při zpracování dat, pokud je to možné, neuvádějí jména ani jiné údaje, podle kterých by mohla být dotyčná osoba identifikována
- zachovávají důvěrnost obsahu veškeré elektronické komunikace a obsahu databází
- jsou si vědomi, že porušení výše uvedených povinností je závažným porušením pracovních povinností
- jsou si vědomi, že zaměstnavatel je po nich oprávněn vymáhat případnou škodu, kterou by porušením výše uvedených povinností způsobili.

Směrnice k využívání IT techniky

Škola	
Směrnice k využívání IT techniky	
Č.j.:	Účinnost od:
Spisový znak:	Skartační znak:
Změny: Číslo: Datum: Změna: Provedl:	

1. Základní ustanovení
   1.1. Tato směrnice je souhrnná vnitřní organizační forma, která určuje zásady využívání, správy, údržby, ochrany a zabezpečení výpočetní techniky, dat a aplikací (dále jen IT).
   1.2. Ustanovení této směrnice jsou závazná pro všechny zaměstnance školy v pracovně právním vztahu a částečně i pro žáky a studenty školy využívající výpočetní techniku (učebna výpočetní techniky, knihovna).

2. Uživatelé
   2.1. Osobní počítače (dále jen PC) jsou ve škole užívány na základě individuální odpovědnosti. Případné technické požadavky sdělují správci informačních technologií (dále jen správce IT), který vede seznam uživatelů IT. Za stav serverů a počítačové sítě odpovídá správce IT.

   2.2. Uživatelé mají právo:
      2.2.1. mít přístup ke svému pc a v něm nainstalovaným programům
      2.2.2. požadavky na konzultace, instalace, nastavení či opravy posílat správci IT
      2.2.3. předkládat pověřeným osobám požadavky na nákup techniky a spotřebního materiálu

   2.3. Uživatelé jsou povinni:
      2.3.1. používat PC pouze pro plnění svých pracovních povinností
      2.3.2. používat jen takové počítačové programy, které jsou ve vlastnictví školy a instalované správcem IT a používat je v souladu s jejich licenčními podmínkami
      2.3.3. hlásit správci IT nalezené závady, potřebné opravy, údržbu nebo žádosti o aktualizaci počítačových programů, nalezení viru, opakovaná chybová hlášení či podezřelé chování PC

2.3.4. při odesílání emailů s obsahem vyžadujícím šifrování použít vhodné šifrovací nástroje
2.3.5. při práci v cloudovém prostředí (emailová komunikace, nahrávání a sdílení dat) dodržovat, že k osobním údajům budou mít přístup pouze oprávněné osoby
2.3.6. provádět pravidelnou zálohu svých dat
2.3.7. před každým použitím externího média (zejména USB) provést kontrolu antivirovým nástrojem
2.3.8. obstarávat si spotřební materiál od pověřené osoby (tonery, papíry)
2.3.9. při práci se služebními notebooky mimo prostory Organizace, v případě odesílání dat s obsahem vyžadujícím šifrování, použít vhodné šifrovací nástroje
2.3.10. odhlásit se z PC před odchodem z pracoviště nebo jej zamknout (Win + L), a to i při přerušení práce, pokud PC zůstane na pracovišti neuzamčeném nebo s přístupem více osob
2.3.11. po skončení práce vypnout PC
2.3.12. při opuštění pracoviště musejí být veškeré papírové dokumenty a média pro ukládání dat obsahující citlivé údaje osobního charakteru odstraněny z pracovního stolu nebo jiných míst (tiskárny, kopírky, skenery apod.), aby se zabránilo neoprávněnému přístupu k nim.

2.4. Uživatelům je výslovně zakázáno:
2.4.1. data a informace s klasifikací “s omezeným přístupem” a další citlivé informace osobního charakteru ukládat na přenosná externí média (např. USB)
2.4.2. data a informace s klasifikací “s omezeným přístupem” a další citlivé informace osobního charakteru vynášet mimo organizaci
2.4.3. přemísťovat PC bez konzultace se správcem IT, měnit připojení internetových zásuvek, telefonů a tiskáren, zakrývat větrací otvory PC, odstraňovat kryty PC a zasahovat do hardware
2.4.4. zasahovat do instalace počítačových programů, měnit konfiguraci, příkazové soubory nebo adresáře potřebné pro chod systému
2.4.5. instalovat či mazat jakékoliv počítačové programy a to ani vlastněné uživatelem, volně šiřitelné, ani stažené z internetu
2.4.6. šířit počítačové programy a používat či poskytnout jakékoliv neoprávněně získané prostředky (licenční kódy, hardwarové klíče) sloužící k ochraně počítačových programů
2.4.7. provádět nezodpovědnou nebo dokonce zlomyslnou činnost na internetu (rozesílání spamů, šíření virů, přetěžování sítí masívním nebo trvalým downloadem či uploadem nebo generováním útoků na webové služby či databáze)

3. Správce IT
3.1. Správce IT provádí:
3.1.1. správu a evidenci uživatelů, nastavování jejich přístupových práv
3.1.2. instalaci a údržbu serverů sítě, technických prostředků sítě, rozvodů sítě a spojení s internetem
3.1.3. instalaci a konfiguraci síťového systémového software, databází a síťového aplikačního software

3.1.4. zálohování dat uložených na serverech počítačové sítě, jednou ročně testem ověřit obnovu dat ze zálohy
3.1.5. hardwarovou instalaci, rozšíření, modernizaci a konfiguraci PC
3.1.6. instalaci a konfiguraci operačního systému PC a dalšího softwarového vybavení PC
3.1.7. evidenci počítačových programů, evidenci oprávněnosti užívat programy (licenční smlouvy) a evidenci o provedených instalacích programů
3.1.8. návrhy nákupů IT techniky (serverů, PC, tiskáren, počítačových programů, hardware), opravy IT (posuzování jejich potřebnosti a rentability) a školení zaměstnanců v oblasti IT

3.2. Správce IT má právo:
3.2.1. přistupovat do PC uživatelů za účelem kontroly a servisu zařízení
3.2.2. při rozhodování o prioritách řešení IT požadavků upřednostňovat požadavky související s obecným zájmem školy (počítačové sítě, servery) před požadavky na jednotlivých pracovištích (lokální PC)
3.2.3. po analýze požadavku zvolit optimální řešení s ohledem na ekonomickou a časovou náročnost
3.2.4. odmítnout nestandartní požadavky uživatelů, které nejsou v souladu s obecnými IT zájmy školy, či kolidují s příslušnými právními předpisy a nařízeními (licenční politika)

4. Ochrana dat (GDRP)
4.1. Všichni zaměstnanci školy jsou povinni:
4.1.1. zachovávat mlčenlivost o údajích, se kterými se seznámí při práci se soubory, databázemi či informačními systémy, nevyzrazovat nikomu své přístupové údaje
4.1.2. zachovávat mlčenlivost o všech dalších skutečnostech, o nichž se dozvědí v souvislosti s výkonem práce v rámci svého pracovního poměru ve škole
4.1.3. zachovávat mlčenlivost o všech těchto skutečnostech i po skončení jejich pracovního poměru ve škole
4.1.4. zachovávat mlčenlivost o osobních údajích, včetně údajů citlivých, a o bezpečnostních opatřeních, jejichž zveřejnění by mohlo ohrozit zabezpečení těchto údajů
4.1.5. výše uvedené skutečnosti a údaje nesdělovat třetím osobám, nedovolit přístup neoprávněných osob k těmto údajům, neohrozit ztrátu těchto údajů
4.1.6. skutečnosti chráněné školským zákonem (§ 28) a osobní údaje zpracovávat jen se souhlasem zaměstnavatele a za účelem, který zaměstnavatel stanoví
4.1.7. při zpracování dat, pokud je to možné, neuvádět jména ani jiné identifikační údaje
4.1.8. zachovávat důvěrnost obsahu veškeré elektronické komunikace a obsahu databází
4.1.9. dodržovat mlčenlivost o všech informacích, se kterými přijdou během svého pracovního poměru do styku

4.1.10. být si vědomi, že porušení těchto výše uvedených povinností je závažným porušením pracovních povinností
4.1.11. být si vědomi, že zaměstnavatel je po nich oprávněn vymáhat případnou škodu, kterou porušením výše uvedených povinností způsobí
4.1.12. v případě úniku/ztráty/zničení dat okamžitě hlásit tuto skutečnost IT správci a pověřenci GDPR

5. Subjekty, jejichž osobní údaje jsou zpracovávány, mají následující práva:
   5.1. Právo na přístup k osobním údajům
   5.2. Právo na opravu, resp. doplnění
   5.3. Právo na výmaz
   5.4. Právo na omezení zpracování
   5.5. Právo na přenositelnost údajů
   5.6. Právo vznést námitku

Kamerové systémy

Účel instalace kamerového systému
Účelem instalace kamerového systému je monitoring vstupních veřejných prostor školy za účelem ochrany zdraví a života. Dále se týká ochrany majetku před krádeží a vandalismem. Tohoto účelu nelze dosáhnout jinými prostředky. Prostory jsou rozsáhlé, členité a pohyb osob značný.

Časový rámec pro ukládání informací
Kamerové systémy jsou vybaveny automatickým záznamovým zařízením (NVR). Nahraný záznam starší 3 dnů je automaticky odstraněn.

Informovanost o nasazení kamer
Všechny snímané prostory jsou označeny informačními nálepkami formátu A5, které jsou umístěny před snímanými prostorami a uvnitř těchto prostor.

Přístup k nahrávaným záznamům
Přístup je umožněn pouze vymezenému okruhu pověřených osob. Tyto osoby se pohybují v rámci zvláštního režimu oprávněných osob, který jasně definuje jejich povinnosti v souvislosti s přístupem k zaznamenávaným údajům. Data nebudou předána třetí osobě, vyjma situací definovaných zákonem.

Směrnice o provozování kamerového systému

Škola	
Směrnice o provozování kamerového systému	
Č.j.:	Účinnost od:
Spisový znak:	Skartační znak:
Změny: Číslo: Datum: Změna: Provedl:	

Základní ustanovení:

1. Tato směrnice se vydává na základě ustanovení § 316 zákona č. 262/2006 Sb., zákoník práce, nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a § 29, odst. 2 zákona č. 561/2004 Sb., školský zákon.
2. Tato směrnice je závazná pro všechny zaměstnance školy, také pro další osoby, které jsou ke škole v jiném pracovně právním vztahu (dohoda o provedení práce, dohoda o pracovní činnosti) nebo v jiném právním vztahu (smlouva o dílo, nájemní smlouva). Zaměstnanec nastupující do pracovního poměru musí být seznámen s tímto vnitřním předpisem před svým nástupem do práce.
3. Svými důsledky se tato směrnice dotýká i žáků, studentů, zákonných zástupců žáků a dalších návštěvníků školy.

Obecné podmínky provozování kamerového systému:

1. Účelem instalace kamerového systému je monitoring vstupních veřejných prostor školy za účelem ochrany zdraví a života. Dále se týká ochrany majetku před krádeží a vandalismem. Tohoto účelu nelze dosáhnout jinými prostředky. Prostory jsou rozsáhlé, členité a pohyb osob značný.
2. Všechny osoby jsou při vstupu do monitorovaných prostor i uvnitř nich na přítomnost kamerového systému upozorněny nálepkami formátu A5.

Způsob zpracovávání osobních údajů:

1. Jednotlivé kamery jsou umístěné ve vstupních prostorách školy a dále ve vnějších prostorách (zadní trakt).
2. Záznamy kamerového systému jsou Organizací uchovávány po dobu 3 dnů, což je nezbytná doba, která slouží k odhalení konkrétního protiprávního jednání.
3. Kamerový systém je zaměstnavatelem používán pouze v určených veřejných prostorách školy.

4. Záznamy kamerového systému jsou chráněny před přístupem neoprávněných osob, před zničením či zneužitím celého systému nebo záznamů.
5. Prostory, které jsou ve škole monitorovány, jsou označeny zřetelným nápisem umístěným v monitorovaných prostorách a před nimi.

Zveřejňování osobních údajů žáků a studentů na internetu

Zpracování osobních údajů

Při zákonném zpracování osobních údajů vychází Organizace především ze zákona 561/2004 Sb., školský zákon. Jedná se o základní zásadu obsaženou čl. 5 nařízení, která říká, že s osobními údaji je třeba zacházet na základě právního důvodu transparentně, se zřetelem ke stanovenému účelu zpracování, a pouze v nezbytném rozsahu.
Využití údajů je možné pouze se souhlasem žáků, resp. jejich zákonných zástupců (to v návaznosti na splnění podmínky rozumové a volní vyspělosti nezletilého (§ 31 občanského zákoníku).
Souhlas subjektu údajů (žák, zákonný zástupce žáka, student, zaměstnanec školy) musí být informovaný, konkrétní a písemný a správce osobních údajů je povinen jej získat ještě předtím, než zpracování osobních údajů zahájí, a také je povinen jej po celou dobu zpracování prokázat.

Směrnice pro zveřejňování osobních údajů žáků a studentů na internetu

Fotografie a videozáznamy

Mezi osobní údaje patří fotografické záznamy a videozáznamy (dále jen fotografie). Činnost školy je neodmyslitelně spojena s pořizováním fotografií žáků, studentů i zaměstnanců školy, popř. dalších osob (zákonní zástupci žáků, účastníci kurzů apod.). Tuto problematiku řeší zákon č. 89/2012 Sb., občanský zákoník.

Pořizování fotografií za účelem propagace a informování o činnosti školy

Při pořizování takových fotografií je nezbytný souhlas žáků a studentů.

Text souhlasu žáka a studenta:
Souhlasím po dobu školního roku x/y se zveřejněním svých fotografií pořízených během akcí školy na webových stránkách školy, pokud nebude má podobizna spojena s mým jménem. Tento souhlas lze kdykoliv odvolat, popř. omezit na konkrétní případy.
Já xy dávám výslovný souhlas ke zpracování těchto mých osobních údajů, a to pro účel propagace školy a její činnosti na webových stránkách školy VOŠZ a SŠZ, Palachova 35, Ústí nad Labem po celou dobu mého studia. Tento souhlas lze kdykoliv odvolat, popř. omezit na konkrétní případy.

Pořizování fotografií mobilními telefony a dalšími zařízeními ze strany žáků a studentů

Text ve školním řádu:
"Žáci a studenti mají během vyučování vypnuté mobilní telefony, fotoaparáty a jinou záznamovou techniku, která slouží k pořizování obrazových a zvukových záznamů. Pořizování zvukových a obrazových záznamů osob (učitel, žák, student) bez jejich svolení je v rozporu s občanským zákoníkem (§ 84 a § 85). Narušování vyučovacího procesu mobilním telefonem (případně jinou technikou), bude hodnoceno jako přestupek proti školnímu řádu."

Oprávněné zpracování osobních údajů - fotografií

Dle ustanovení občanského zákoníku (Podoba a soukromí, § 84 až § 90), platí:

1. Do práva na soukromí nezasahuje ten (roz. oprávněně zpracovává osobní údaje a případně je dále používá ten), kdo pořizuje osobní údaje (např. fotografie) za účelem výkonu nebo ochrany práv a osob. Jako příklad lze uvést pořízení nebo použití fotografií nebo záznamů o šikaně nebo jiném protiprávním jednání, dokumentace úrazů apod.
2. Záznam nebo fotografie se pořizuje k úřednímu účelu, např. při styku s rodiči v souvislosti s řešením stížností, závažných výchovných nebo vzdělávacích otázek spojených s konkrétním žákem apod.
3. Dalším oprávněným zásahem do soukromí (tedy povoleným zpracováváním osobních údajů jejich pořízením nebo použitím) jsou tzv. vědecké, umělecké nebo zpravodajské licence (např. oprávnění novináře natáčet i bez souhlasu). Jako příklad lze uvést pořizování fotografií z veřejných akcí pořádaných školou pro novinářské či reportážní účely (např. do školních novin). Zpravodajská licence se nevztahuje na pořizování fotografií výhradně za účelem propagace či zvýšení zájmů žáků a studentů o studium. Proto je třeba u jednotlivých fotografií odlišovat, zda je fotografována konkrétní osoba, která o pořizování snímků své osoby ví, konkludentně s ní souhlasí (např. pózuje a nic nenamítá) a zároveň ví, jak bude s fotografií nakládáno, nebo zda je pořizována fotografie velké skupiny osob pouze pro ilustrační účely. Zde není z povahy věci třeba trvat na souhlasu osob, jestliže není možné jednotlivé osoby rozpoznat.
4. Všechny zákonné výjimky musí být využívány přiměřeným způsobem, v souladu s pravidly slušnosti a obvyklého chování v občanské společnosti (preambule Ústavy).

Bezpečnostní nástroje Organizace

Cloud computing

Při práci s citlivými údaji osobního charakteru musí být ze strany uživatelů dodržováno, že osobní údaje musejí být přístupné pouze oprávněným osobám.

Zálohování

Zálohování serverů probíhá automaticky dle nastaveného schématu. Zálohování dat v osobních počítačích si uživatelé zajišťují samostatně.

Antivirová ochrana

Antivirový software musí být nainstalován v každém počítači a musí mít aktivován automatické aktualizace. Uživatel není oprávněn měnit nastavení antivirového SW. Antivirovým nástrojem jsou vybaveny i všechny servery.

Řízení přístupů

Každý uživatel má přístup do svého uživatelského účtu. Účty jsou nastaveny bez administrátorského oprávnění. Při změně pracovní pozice jsou oprávnění upravena. Nejsou používány anonymní účty nebo účty typu host.

Řízení hesel

Uživatelské účty zaměstnanců musejí být opatřeny heslem. V případě podezření z manipulace s heslem, musí být heslo změněno.

Přenos dat

Přenos dat typu “s omezeným přístupem” je možný pouze v zašifrované podobě (protokoly typu https, ftps, atd.) nebo prostřednictvím datové schránky.

Ochrana sítě

Vnitřní síť je od vnější oddělena firewallem. Dále je aplikována segmentace sítí tak, aby byly od sebe odděleny na L2 nebo L3 vrstvě servery vystavené do internetu, interní servery a počítače uživatelů.

Vzdálená správa (VPN)

Vzdálená správa počítačů je prováděna vždy prostřednictvím zabezpečeného připojení a šifrovaným kanálem.

Mobilní zařízení

Pokud se v mobilních zařízeních vyskytují informace zařazené do kategorie “s omezeným přístupem”, pak je možné toto zařízení na dálku spravovat.

Logování

Všechny kritické prvky síťové infrastruktury jsou logovány. Je možné až 3 měsíce zpětně dohledat veškeré proběhlé operace.

Fyzická bezpečnost

IT technika, která obsahuje data “s omezeným přístupem” je uložena v uzamykatelné místnosti v kontrolovatelným vstupem.

Tisk dokumentů

Autor tisku musí mít tištěný dokument obsahující data “s omezeným přístupem” pod kontrolou od okamžiku tisku až po jeho vyzvednutí z tiskárny.

SDĚLENÍ PRO ŽÁKY A STUDENTY

SMĚRNICE ZÁSAD OCHRANY OSOBNÍCH ÚDAJŮ PRO ŽÁKY A STUDENTY

Pravidla pro užívání IT
Pro uživatele jsou stanovena následující pravidla:

- IT technika VOŠZ a SŠZ, Palachova 35, Ústí nad Labem (dále jen „Organizace“) se užívá dle zásad osobní odpovědnosti
- po skončení práce se musejí odhlásit od všech aplikací
- PC a další koncová zařízení se užívají pouze pro výkon studijních povinností určených vyučujícími
- žáci a studenti užívají pouze takové systémy a aplikace, které jsou licencované v rámci školy a instalované správcem IT
- vyučujícímu jsou hlášeny nalezené závady, zjištěné chyby a nestandartní chování používaného zařízení
- před každým použitím externího média (zejména USB), je toto médium prověřeno antivirovým nástrojem
- při práci v cloudovém prostředí (emailová komunikace, nahrávání a sdílení dat) žáci a studenti dodržují, aby k jejich osobním údajům měly přístup pouze oprávněné osoby
- uživatelé zachovávají mlčenlivost ohledně svých přístupových údajů do aplikací a dalších systémů
- nesdělovat nikomu své přístupové údaje do programu Bakaláři; v případě porušení tohoto bodu se správce zříká jakékoli odpovědnosti

Uživatelům je zakázáno:

- přenášet koncové zařízení bez souhlasu vyučujícího
- zasahovat do operačního systému a instalovaných aplikací
- měnit systémovou konfiguraci a strukturu adresářů OS
- instalovat či odinstalovávat jakékoliv školní aplikace, včetně volně šiřitelných z internetu
- dále šířit jakékoliv školní aplikace, včetně licenčních kódů a HW klíče
- provádět nezodpovědnou nebo dokonce zlomyslnou činnost na internetu (rozesílání spamů, šíření virů, přetěžování sítí masívním nebo trvalým downloadem či uploadem nebo generováním útoků na webové služby či databáze
- přistupovat do programu Bakaláři ze zařízení, které není bezpečně chráněno antivirovým programem

Zveřejňování osobních údajů žáků a studentů na internetu

Zpracování osobních údajů
Při zákonném zpracování osobních údajů vychází Organizace především ze zákona 561/2004 Sb., školský zákon. Jedná se o základní zásadu obsaženou čl. 5 nařízení, která říká, že

s osobními údaji je třeba zacházet na základě právního důvodu transparentně, se zřetelem ke stanovenému účelu zpracování, a pouze v nezbytném rozsahu.
Využití údajů je možné pouze se souhlasem žáků, resp. jejich zákonných zástupců (to v návaznosti na splnění podmínky rozumové a volní vyspělosti nezletilého (§ 31 občanského zákoníku).
Souhlas subjektu údajů (žák, zákonný zástupce žáka, student) musí být informovaný, konkrétní a písemný a správce osobních údajů je povinen jej získat ještě předtím, než zpracování osobních údajů zahájí, a také je povinen jej po celou dobu zpracování prokázat.

Fotografie a videozáznamy
Mezi osobní údaje patří fotografické záznamy a videozáznamy (dále jen fotografie). Činnost školy je neodmyslitelně spojena s pořizováním fotografií žáků, studentů i zaměstnanců školy, popř. dalších osob (zákonní zástupci žáků, účastníci kurzů apod.). Tuto problematiku řeší zákon č. 89/2012 Sb., občanský zákoník.

Pořizování fotografií za účelem propagace a informování o činnosti školy
Při pořizování takových fotografií je nezbytný souhlas žáků a studentů.

Text souhlasu žáka a studenta:
Souhlasím po dobu školního roku x/y se zveřejněním svých fotografií pořízených během akcí školy na webových stránkách školy, pokud nebude má podobizna spojena s mým jménem. Tento souhlas lze kdykoliv odvolat, popř. omezit na konkrétní případy.
Já xy dávám výslovný souhlas ke zpracování těchto mých osobních údajů, a to pro účel propagace školy a její činnosti na webových stránkách školy VOŠZ a SŠZ, Palachova 35, Ústí nad Labem po celou dobu mého studia. Tento souhlas lze kdykoliv odvolat, popř. omezit na konkrétní případy.

Pořizování fotografií mobilními telefony a dalšími zařízeními ze strany žáků a studentů
Školní řád stanovuje:
"Žáci a studenti mají během vyučování vypnuté mobilní telefony, fotoaparáty a jinou záznamovou techniku, která slouží k pořizování obrazových a zvukových záznamů. Pořizování zvukových a obrazových záznamů osob (učitel, žák, student) bez jejich svolení je v rozporu s občanským zákoníkem (§ 84 a § 85). Narušování vyučovacího procesu mobilním telefonem (případně jinou technikou), bude hodnoceno jako přestupek proti školnímu řádu."

Oprávněné zpracování osobních údajů - fotografií
Dle ustanovení občanského zákoníku (Podoba a soukromí, § 84 až § 90), platí:

1. Do práva na soukromí nezasahuje ten (roz. oprávněně zpracovává osobní údaje a případně je dále používá ten), kdo pořizuje osobní údaje (např. fotografie) za účelem výkonu nebo ochrany práv a osob. Jako příklad lze uvést pořízení nebo použití fotografií nebo záznamů o šikaně nebo jiném protiprávním jednání, dokumentace úrazů apod.
2. Záznam nebo fotografie se pořizuje k úřednímu účelu, např. při styku s rodiči v souvislosti s řešením stížností, závažných výchovných nebo vzdělávacích otázek spojených s konkrétním žákem apod.
3. Dalším oprávněným zásahem do soukromí (tedy povoleným zpracováváním osobních údajů jejich pořízením nebo použitím) jsou tzv. vědecké, umělecké nebo zpravodajské licence (např. oprávnění novináře natáčet i bez souhlasu). Jako příklad lze uvést

pořizování fotografií z veřejných akcí pořádaných školou pro novinářské či reportážní účely (např. do školních novin). Zpravodajská licence se nevztahuje na pořizování fotografií výhradně za účelem propagace či zvýšení zájmů žáků a studentů o studium. Proto je třeba u jednotlivých fotografií odlišovat, zda je fotografována konkrétní osoba, která o pořizování snímků své osoby ví, konkludentně s ní souhlasí (např. pózuje a nic nenamítá) a zároveň ví, jak bude s fotografií nakládáno, nebo zda je pořizována fotografie velké skupiny osob pouze pro ilustrační účely. Zde není z povahy věci třeba trvat na souhlasu osob, jestliže není možné jednotlivé osoby rozpoznat.

4. Všechny zákonné výjimky musí být využívány přiměřeným způsobem, v souladu s pravidly slušnosti a obvyklého chování v občanské společnosti (preambule Ústavy).

SDĚLENÍ PRO ZÁKONNÉ ZÁSTUPCE

SMĚRNICE ZÁSAD OCHRANY OSOBNÍCH ÚDAJŮ PRO ZÁKONNÉ ZÁSTUPCE

Pravidla pro užívání IT:

- zákaz přístupu do programu Bakalář ze zařízení, které není bezpečně chráněno antivirovým programem
- nesdělovat nikomu své přístupové údaje do programu Bakaláři; v případě porušení tohoto bodu se správce zříká jakékoli odpovědnosti

---

Zveřejňování osobních údajů žáků a studentů na internetu

Zpracování osobních údajů

Při zákonném zpracování osobních údajů vychází VOŠZ a SŠZ, Palachova 35, Ústí nad Labem (dále jen „Organizace“) především ze zákona 561/2004 Sb., školský zákon. Jedná se o základní zásadu obsaženou čl. 5 nařízení, která říká, že s osobními údaji je třeba zacházet na základě právního důvodu transparentně, se zřetelem ke stanovenému účelu zpracování, a pouze v nezbytném rozsahu.
Využití údajů je možné pouze se souhlasem žáků, resp. jejich zákonných zástupců (to v návaznosti na splnění podmínky rozumové a volní vyspělosti nezletilého (§ 31 občanského zákoníku).
Souhlas subjektu údajů (žák, zákonný zástupce žáka, student) musí být informovaný, konkrétní a písemný a správce osobních údajů je povinen jej získat ještě předtím, než zpracování osobních údajů zahájí, a také je povinen jej po celou dobu zpracování prokázat.

Fotografie a videozáznamy

Mezi osobní údaje patří fotografické záznamy a videozáznamy (dále jen fotografie). Činnost školy je neodmyslitelně spojena s pořizováním fotografií žáků, studentů i zaměstnanců školy, popř. dalších osob (zákonní zástupci žáků, účastníci kurzů apod.). Tuto problematiku řeší zákon č. 89/2012 Sb., občanský zákoník.

Pořizování fotografií za účelem propagace a informování o činnosti školy

Při pořizování takových fotografií je nezbytný souhlas žáků a studentů.

Text souhlasu žáka a studenta:
Souhlasím po dobu školního roku x/y se zveřejněním svých fotografií pořízených během akcí školy na webových stránkách školy, pokud nebude má podobizna spojena s mým jménem. Tento souhlas lze kdykoliv odvolat, popř. omezit na konkrétní případy.
Já xy dávám výslovný souhlas ke zpracování těchto mých osobních údajů, a to pro účel propagace školy a její činnosti na webových stránkách školy VOŠZ a SŠZ, Palachova 35, Ústí

nad Labem po celou dobu mého studia. Tento souhlas lze kdykoliv odvolat, popř. omezit na konkrétní případy.

Pořizování fotografií mobilními telefony a dalšími zařízeními ze strany žáků a studentů

Školní řád stanovuje:

"Žáci a studenti mají během vyučování vypnuté mobilní telefony, fotoaparáty a jinou záznamovou techniku, která slouží k pořizování obrazových a zvukových záznamů. Pořizování zvukových a obrazových záznamů osob (učitel, žák, student) bez jejich svolení je v rozporu s občanským zákoníkem (§ 84 a § 85). Narušování vyučovacího procesu mobilním telefonem (případně jinou technikou), bude hodnoceno jako přestupek proti školnímu řádu."

Oprávněné zpracování osobních údajů - fotografií

Dle ustanovení občanského zákoníku (Podoba a soukromí, § 84 až § 90), platí:

5. Do práva na soukromí nezasahuje ten (roz. oprávněně zpracovává osobní údaje a případně je dále používá ten), kdo pořizuje osobní údaje (např. fotografie) za účelem výkonu nebo ochrany práv a osob. Jako příklad lze uvést pořízení nebo použití fotografií nebo záznamů o šikaně nebo jiném protiprávním jednání, dokumentace úrazů apod.
6. Záznam nebo fotografie se pořizuje k úřednímu účelu, např. při styku s rodiči v souvislosti s řešením stížností, závažných výchovných nebo vzdělávacích otázek spojených s konkrétním žákem apod.
7. Dalším oprávněným zásahem do soukromí (tedy povoleným zpracováváním osobních údajů jejich pořízením nebo použitím) jsou tzv. vědecké, umělecké nebo zpravodajské licence (např. oprávnění novináře natáčet i bez souhlasu). Jako příklad lze uvést pořizování fotografií z veřejných akcí pořádaných školou pro novinářské či reportážní účely (např. do školních novin). Zpravodajská licence se nevztahuje na pořizování fotografií výhradně za účelem propagace či zvýšení zájmů žáků a studentů o studium. Proto je třeba u jednotlivých fotografií odlišovat, zda je fotografována konkrétní osoba, která o pořizování snímků své osoby ví, konkludentně s ní souhlasí (např. pózuje a nic nenamítá) a zároveň ví, jak bude s fotografií nakládáno, nebo zda je pořizována fotografie velké skupiny osob pouze pro ilustrační účely. Zde není z povahy věci třeba trvat na souhlasu osob, jestliže není možné jednotlivé osoby rozpoznat.
8. Všechny zákonné výjimky musí být využívány přiměřeným způsobem, v souladu s pravidly slušnosti a obvyklého chování v občanské společnosti (preambule Ústavy).