SMĚRNICE NA OCHRANU OSOBNÍCH ÚDAJŮ a ICT BEZPEČNOST

Název organizace: Střední škola řemesel a služeb, Děčín IV, Ruská 147, p.o.

Platnost od: 1. 3. 2021

Počet stran:

Tato směrnice je v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů a v souladu s Nařízením Evropského parlamentu a rady (EU) č. 2016/679, 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 „Nařízení“) tento vnitřní předpis je využíván pro potřeby naší organizace (dále jen „směrnice“):

Čl 1. Předmět směrnice

1. Tato směrnice upravuje postupy školy, jejich zaměstnanců, případně dalších osob při nakládání s osobními údaji, pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchování osobních údajů a ICT bezpečnosti. Směrnice rovněž upravuje některé povinnosti školy, jejich zaměstnanců, případně dalších osob při nakládání s osobními údaji.
2. Ustanovení této směrnice jsou závazná pro všechny zaměstnance.
3. Touto směrnicí jsou dále stanoveny vnitřní pravidla pro:
    a. užívání výpočetní techniky (hardware) a programového vybavení (software)
    b. užívání počítačové sítě školy včetně všech počítačů a dalších technických zařízení (tiskárny, modemy, scannery, rozvaděče atd.), které jsou přímo nebo prostřednictvím jiného zařízení funkčně připojeny k počítačové síti školy
    c. informační a datovou bezpečnost, včetně ochrany a zálohování elektronických dat a nakládání s hesly (heslová politika)
    d. používání služeb internetu a elektronické pošty
    e. zpracování osobních údajů ve školní matrice v listinné a elektronické podobě.
4. Zásadním dokumentem, který stanoví závazné právní vztahy všech stran, jejich součinnost a postavení při ochraně osobních údajů, je školní řád. Aktuální verze školní

řádu je dostupná na webu organizace nebo u ředitele. Neznalost školní řádu neomlouvá.

Čl 2. Základní pojmy, technické pojmy a zkratky

Pro účely této směrnice se rozumí

a. **osobním údajem** jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,
b. **citlivým údajem** osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,
c. **zpracováním osobních údajů** jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,
d. **zpracovatelem fyzická nebo právnická osoba**, nebo subjekt, který zpracovává osobní údaje pro správce (správce si jej najímá – účetní, lékař…),
e. **správcem právnická nebo fyzická osoba**, která určuje účely a prostředky zpracování osobních údajů,
f. **pověřencem osoba**, která posuzuje činnost správce či zpracovatele, zda je v souladu s platnou právní úpravou, informuje je, radí, dává doporučení,
g. **subjektem údajů fyzická osoba**, k níž se osobní údaje vztahují,
h. **souhlasem subjektu údajů** svobodný, konkrétní, informovaný, jednoznačný, jasný a prokazatelný vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.
i. **počítačová síť školy** (dále jen „síť“) – všechna technická zařízení a programové vybavení používané při činnosti orgánů školy v budovách školy k vzájemnému technickému a datovému propojení počítačů, síť spolu s přímo nebo nepřímo na síť připojenými počítači a jinými technickými zařízeními a programovým vybavením tvoří **počítačový systém školy** (dále jen „systém“)
j. **počítač** (dále jen „PC“) – počítač ve vlastnictví školy nebo oprávněně školou užívaný a připojený do sítě případně fungující samostatně mimo síť

k. **výpočetní technika školy** (dále jen „výpočetní technika“) – všechny PC, ostatní zařízení informační techniky a všechny technické součásti sítě, které jsou ve vlastnictví nebo v oprávněném užívání školy a jsou využívána při činnosti orgánů školy
l. **programové vybavení** (dále jen „programy“) – programy a aplikace ve vlastnictví nebo v oprávněném užívání školy, které jsou využívány při provozu výpočetní techniky
m. **uživatel** – zaměstnanec, který je oprávněn užívat výpočetní techniku a programy
n. **uživatelské oprávnění** – oprávnění uživatele ve vymezeném rozsahu užívat výpočetní techniku a programy; podmínky vzniku uživatelského oprávnění stanoví tato směrnice
o. **uživatelský účet** – fyzické vyjádření uživatelského oprávnění; základními parametry jsou uživatelské jméno (login), heslo (password), definice přístupových práv a e-mailová adresa uživatele
p. **správce sítě** – zabezpečuje podle této směrnice provoz výpočetní techniky, systému, sítě a další úkoly stanovené touto směrnicí.

Kategorie A
Oblast ochrany osobních údajů

Čl 3. Zásady nakládání s osobními údaji

Při nakládání s osobními údaji se škola, její zaměstnanci a další osoby řídí těmito zásadami:

a. Postupovat při nakládání s osobními údaji v souladu s právními předpisy,
b. S osobními údaji nakládat uvážlivě, souhlas se zpracováním osobních údajů nenadužívat,
c. Zpracovávat osobní údaje ke stanovenému účelu a ve stanoveném rozsahu a dbát na to, aby tyto byly pravdivé a přesné,
d. Zpracovávat osobní údaje v souladu se zásadou zákonnosti – na základě právních předpisů, při plnění ze smlouvy, při plnění právní povinnosti správce, při ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (zejména děti požívají vyšší ochrany), při ochraně oprávněných zájmů školy, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,
e. Respektovat práva člověka, který je subjektem údajů, zejména práva dát a odvolat souhlas se zpracováním, práva na výmaz, namítat rozsah zpracování apod.,
f. *Poskytovat při zpracování osobních údajů zvláštní ochranu dětem,
g. Poskytovat informace o zpracování osobních údajů, komunikovat,
h. Při uzavírání smluv a právním jednání postupovat se zřetelem na povinnost chránit osobní údaje před zneužitím,
i. Spolupracovat s pověřencem pro ochranu osobních údajů.

Čl 4. Postupy školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji

1. Škola všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Přitom škola především uchovává osobní údaje v prostorách, na místech, v prostředí nebo v systému, do kterého má přístup omezený, předem stanovený a v každý okamžik alespoň řediteli školy známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením ředitele školy nebo jím pověřené osoby.
2. Škola zavede taková opatření, aby o nakládání a zpracování osobních údajů měl přehled alespoň ředitel školy nebo jím pověřená osoba a pověřenec pro ochranu osobních údajů. Mezi tato opatření patří např. ústní nebo písemná informace, písemná komunikace, stanovení povinností v pracovní smlouvě, v dohodě o provedení práce, v dohodě o pracovní činnosti, ve smlouvě, kterou škola uzavírá se třetí osobou (nájemní smlouva, smlouva o dílo, smlouva o poskytování služeb).
3. Škola alespoň jednou za rok provede zhodnocení postupů při nakládání a zpracování osobních údajů. Zhodnocení může být provedeno dle zvyklostí školy, zpravidla se učiní stručný záznam např. v zápisu z porady. Zjistí-li se, že některé postupy školy jsou zastaralé, zbytečné nebo se neosvědčily, učiní škola bezodkladně nápravu.
4. Každý zaměstnanec školy při nakládání s osobními údaji respektuje jejich povahu, tedy že jde o součást soukromí člověka jako subjektu údajů, a tomu přizpůsobí úkony s tím spojené.
5. Zaměstnanec zejména osobní údaje nezveřejňuje bez ověření, že takový postup je možný, nezpřístupňuje osobní údaje osobám, které neprokáží právo s nimi nakládat.
6. Zaměstnanec, vyplývá-li taková povinnost z jiných dokumentů, informuje subjekt údajů o jeho právech na ochranu osobních údajů; jinak odkáže na ředitele školy nebo jím určenou osobu nebo na pověřence pro ochranu osobních údajů.
7. Škola při nakládání a zpracovávání osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů.
8. Škola ihned řeší každý bezpečnostní incident týkající se osobních údajů, a to v součinnosti s pověřencem pro ochranu osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, především konkrétního žáka, studenta, zaměstnance, zákonného zástupce atd., škola tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepíše záznam. O každém závažném incidentu škola informuje Úřad pro ochranu osobních údajů.

Čl 5. Organizační opatření k ochraně osobních údajů ve škole

1. Třídní výkazy, katalogové listy a další materiály ze školní matriky, které obsahují osobní údaje žáků, jsou trvale uloženy v uzamykatelných skříních v kanceláři školy, a to v kanceláři zástupce ředitele školy. Třídním učitelům jsou zapůjčeny na nezbytně dlouhou dobu k provedení zápisů. Třídní výkazy, katalogové listy, další materiály ze školní matriky či jejich části nelze vynášet ze školy, předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.
2. V organizaci je stanoven klíčový režim, (klíče, přidělené zaměstnancům, jsou evidovány) stejně tak jako v případě pronájmu nebytových prostor v areálu školy. Duplikáty klíčů nejsou na veřejně přístupném místě cizím osobám.
3. Úklid prostor organizace je prováděn vlastními zaměstnanci.
4. Do serverovny a jiných klíčových zařízení je zabráněno vstupu nepovolaným osobám a těmto osobám není dovoleno s těmito zařízeními jakkoliv manipulovat nebo je poškodit.
5. Elektronická školní matrika je vedena v zabezpečeném informačním systému „Bakaláři“. Do tohoto systému mají přístup jednotliví pedagogové školy a další osoby výslovně a písemně pověřené ředitelem školy, a to jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením.
6. Při práci s elektronickou evidencí oprávnění nesmí oprávněné osoby opouštět počítač bez odhlášení se, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přihlašovacího hesla; a v případě nebezpečí jeho vyzrazení jej ihned (ve spolupráci se správcem sítě) změnit. Přístupy nastavuje pověřený zaměstnanec školy – správce počítačové sítě, který nastavuje potřebné zabezpečení dat a školní počítačové sítě (dle pokynů ředitele).
7. Zákonní zástupci žáků a žáci mají zajištěn zabezpečený dálkový přístup výhradně k vlastním údajům o klasifikaci na základě přihlašovacího kódu a hesla předaného správcem počítačové sítě prostřednictvím třídních učitelů a učitelů ICT.
8. Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři mzdové účetní, přístup k nim má ředitel školy nebo zástupce ředitele, zastupuje-li ředitele, případně, je-li to nutné též sekretářka školy nebo mzdová účetní.
9. Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni, zpravidla na poradě.
10. Zaměstnanci školy neposkytují bez právního důvodu žádnou formou osobní údaje zaměstnanců školy a žáků cizím osobám a institucím, tedy ani telefonicky, ani e-mailem, ani při osobním jednání.
11. Písemná hodnocení a posudky, která se odesílají mimo školu, např. pro potřeby soudního řízení, přijímacího řízení, zpracovávají zaměstnanci určení ředitelem školy. Nejsou však oprávněni samostatně tato hodnocení podepisovat, poskytovat a odesílat jménem školy a mají povinnost zachovávat mlčenlivost o dané věci.

12. Seznamy žáků se nezveřejňují, neposkytují bez vědomého souhlasu žáků či zákonných zástupců žáků jiným fyzickým či právnickým osobám nebo orgánům, které neplní funkci orgánu nadřízeného škole nebo nevyplývá-li to ze zákona.
13. V propagačních materiálech školy, ve výroční zprávě či ročence školy, na školním webu či na nástěnkách ve škole apod. lze s obecným souhlasem žáků nebo zákonných zástupců žáků uveřejňovat výhradně textové či obrazové informace o jejich úspěších (např. u soutěží umístění na předních místech) s uvedením pouze jména (případně ročníku či třídy). Při publikování v tisku se autor dotazuje na souhlas příslušného žáka. Žák nebo zákonný zástupce má právo požadovat bezodkladné zablokování či odstranění informace či fotografie či záznamu týkající se jeho osoby, který zveřejňovat nechce a toto platí i v případě uvedení osobní údajů na sociálních sítích organizace, která takový účet má zřízený. Platí to i o fotografiích či záznamech žáka bez uvedení jména v rámci obecné dokumentace školních akcí a úspěchů.
14. Psychologické, lékařské a jiné průzkumy a testování mezi žáky, jejichž součástí by bylo uvedení osobních údajů žáka, lze provádět jen se souhlasem žáka nebo zákonného zástupce žáka. To se netýká anonymních průzkumů, které však musí souviset se vzděláváním na dané škole a musí s ním předem písemně souhlasit ředitel či zástupce ředitele; to platí zvláště v případě, že výsledky jsou poskytovány mimo školu.
    Pokud jsou pro vedení dokumentace využívány formuláře a software, je nutné provést kontrolu, zda nepožadují či nenabízejí evidenci nadbytečných údajů a tyto údaje nezpracovávat.
15. Ve škole se provozují kamerové systémy (bez záznamu dat) sledující vstupní prostory používané žáky a zaměstnanci školy v době, kdy jsou žáci přítomni ve škole.

Čl 6. Pravidla v oblasti ochrany osobních údajů u smluvních vztahů

Uzavírá-li škola jakoukoli smlouvu (nájemní smlouvu, smlouvu o dílo, smlouvu o poskytnutí služeb, nepojmenovanou smlouvu apod.), k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, škola vždy a bezpodmínečně bude trvat na tom, aby ve smlouvě byla druhé smluvní straně uložena povinnost:

a. přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,
b. nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu školy,
c. zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí, mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
d. zajistit, aby se osoby oprávněné zpracovávat osobní údaje u dodavatele byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,

e. zajistit, že dodavatel bude škole bez zbytečného odkladu nápomocen při plnění povinností školy, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje školu,
f. po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí škole a vymaže existující kopie apod.,
g. poskytnout škole veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené škole právními předpisy,
h. umožnit kontrolu, audit či inspekci prováděné školou nebo příslušným orgánem dle právních předpisů,
i. poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví škola, součinnost
j. potřebnou pro plnění zákonných povinností školy spojených s ochranou osobních údajů, jejich zpracováním,
k. poskytnuté osobní údaje chránit v souladu s právními předpisy,

Čl 7. Pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů

1. **Škola nakládá a zpracovává pouze osobní údaje, které:**
    a. souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, se sociálním, a zdravotním pojištěním (např. dosažené vzdělání, délka praxe, funkční zařazení apod.),
    b. souvisejí s jednoznačnou identifikací zákonných zástupců žáků v souladu se zákonem (jméno, příjmení, bydliště, kontakt, např. telefonní číslo pro případ nutného kontaktu školy se zákonným zástupcem v rámci ochrany zdraví, bezpečnosti a práv žáka, další údaje nezbytné např. pro vydání správního rozhodnutí apod.),
    c. související s identifikací žáka ze zákona (datum narození, místo narození, rodné číslo, státní příslušnost, bydliště, údaj o zákonném zástupci, soudní rozhodnutí vztahující se k přidělení dítěte do výchovy, nutný zdravotní údaj apod.),
    d. jsou nezbytné pro plnění právní povinnosti, ochranu oprávněných zájmů školy nebo ve veřejném zájmu, k jejichž zpracování získala souhlas subjektu údajů.
2. **Osobní údaje se uchovávají pouze po dobu, která je nezbytná k dosažení účelu jejich zpracování, včetně archivace.**

3. **K osobním údajům mají přístup osoby k tomu oprávněné zákonem nebo na základě zákona. Do jednotlivých dokumentů školy, které obsahují osobní údaje, mohou nahlížet:**
    a. do osobního spisu zaměstnance vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele (§ 312 zákoníku práce),
    b. do údajů žáka ve školní matrice pedagogičtí pracovníci školy (v rozsahu daném pedagogickou funkcí), ekonom/ka školy do údajů o zdravotním stavu žáka, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv – výchovný poradce, vedoucí pedagogičtí pracovníci, třídní učitel, ekonom/ka školy,
    c. do spisu, vedeném ve správním řízení účastníci správního řízení, vedoucí pedagogičtí pracovníci (ředitel, zástupce ředitele, vedoucí vychovatel), osoba, která je zmocněna s úředním spisem pracovat po dobu řízení,
4. <u>Souhlas k zpracováním osobních údajů:</u>
    a. Ke zpracování osobních údajů nad rozsah vyplývající ze zákonů (ze zákona vyplývá i oprávněný zájem, plnění právní povinnosti, plnění smlouvy, veřejný zájem) je nezbytný souhlas osoby, o jejíž osobní údaje se jedná. Souhlas musí být poučený, informovaný a konkrétní, nejlépe v písemné podobě. Souhlas se získává pouze pro konkrétní údaje (určené např. druhově), na konkrétní dobu a pro konkrétní účel.
    b. Souhlas se získává pro zpracování osobních údajů jen tehdy, pokud je jejich zpracování nezbytně nutné a právní předpisy jiný důvod pro toto zpracování nestanoví.
    c. Souhlas se poskytuje podle účelu např. na celé období školní docházky na škole, na školní rok, na dobu školy v přírodě apod. Udělený souhlas může být v souladu s právními předpisy odvolán.

Čl 8. Práva subjektu údajů

Subjekt údajů má následující práva:

1. **Právo na informace a přístup k osobním údajům –** správce je povinen subjekt údajů informovat o zpracování osobních údajů nejpozději v okamžiku získání osobních údajů. Informace musí být zajištěna v plné šíři dle Nařízení.
2. **Právo na opravu –** subjekt údajů má právo, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje nebo doplnil neúplné osobní údaje. Subjekt údajů má

právo na opravu údajů, pokud jsou nepřesné, nebo neúplné, na provedení opravy nejdéle do jednoho měsíce, na vysvětlení, pokud oprava nebyla provedena.

3. **Právo na výmaz –** subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají. Toto právo svědčí subjektu údajů tehdy, je-li zpracování založeno na souhlasu a dojde-li k jeho odvolání, jestliže zpracování osobních údajů již není potřebné pro vymezené účely, jestliže subjekt údajů vznese námitku proti zpracování osobních údajů založeném na oprávněném či veřejném zájmu a z balančního testu vyplyne, že již neexistují převažující oprávněné zájmy správce a dále pokud je zpracování osobních údajů protiprávní. Výmaz se provádí na základě písemné žádosti.
4. **Právo na omezení zpracování –** subjekt údajů má právo požádat o omezení zpracování osobních údajů, a to tehdy, žádá-li o opravu osobních údajů. Do doby opravy správce pozastaví zpracování osobních údajů. Dalšími důvody omezení zpracování osobních údajů je protiprávní zpracování, správce již osobní údaje pro vymezené účely nepotřebuje, subjekt údajů vznesl námitku proti zpracování a do doby jejího posouzení se osobní údaje nezpracovávají.
5. **Právo na přenositelnost** – svědčí subjektu údajů u osobních údajů zpracovávaných automatizovaně na základě souhlasu nebo smlouvy. V takovém případě správce poskytne subjektu údajů osobní údaje ve strukturovaném běžně používaném a strojově čitelném formátu.
6. **Právo vznést námitku** – má subjekt údajů z důvodů týkajících se zpracování osobních údajů založených na veřejném nebo oprávněném zájmu. V takovém případě správce osobních údajů musí doložit, že oprávněný či veřejný zájem převažuje nad ochranou osobních údajů subjektu, a že je tedy jeho zpracování osobních údajů oprávněné. Doložení se provádí zpracováním balančního testu.
7. **Právo podat stížnost** – každý subjekt údajů má právo podat stížnost u dozorového úřadu, pokud se subjekt údajů domnívá, že zpracováním jeho osobních je porušeno Nařízení.

Čl 9. Pověřenec pro ochranu osobních údajů

1. Činnost pověřence pro ochranu osobních údajů je vykonávána prostřednictvím externí společnosti 2K CONSULTING s.r.o, tato osoba je nahlášená u dozorového úřadu ÚOOU
2. <u>Pověřenec pro ochranu osobních údajů si plní povinnosti dle uzavřeného smluvního vztahu:</u>
    a. poskytuje poradenskou a informační činnost
    b. monitoring dodržování ochrany osobních údajů
    c. provádí kontrolní činnost
    d. zajišťuje školení zaměstnanců formou on-line

e. poskytuje součinnost při ohlášení bezpečnostních incidentů dozorovému úřadu (ÚOOU), případně subjektům údajů, a plni si další povinnosti dle legislativy

Čl 10. Ohlášení bezpečnostních incidentů

1. Organizace je bez zbytečného odkladu, a pokud je to možné do 72 hodin od okamžiku, kdy bylo porušení zabezpečení zjištěno, povinna ohlásit ÚOOÚ porušení zabezpečení osobních údajů, v případě nejvyššího rizika a velkého množství osobních údajů.
2. Organizace dokumentuje veškeré případy porušení zabezpečení osobních údajů, a to tak, aby tato dokumentace umožnila ÚOOÚ ověření souladu s článkem 33 Nařízení GDPR.
3. Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob (a nejsou splněny vylučující podmínky uvedené v článku 34 Nařízení GDPR) oznámí organizace toto porušení bez zbytečného odkladu subjektům údajů.
4. K zajištění výše uvedených povinností ředitel školy ve spolupráci se Správcem ICT, neprodleně nahlásí Pověřenci pro ochranu osobních údajů veškeré vzniklé bezpečnostní incidenty, které se týkají nebo mohou týkat osobních údajů.

Kategorie B
Informační a datová bezpečnost / ICT Bezpečnost

Čl 11. Základní povinnosti a oprávnění ICT Bezpečnost

1. Uživatel je oprávněn užívat výpočetní techniku, síť a programy v rozsahu svého uživatelského oprávnění a přístupových práv. Uživatel je povinen respektovat pokyny správce sítě, které vydá v souladu se svými oprávněními a povinnostmi.
2. Uživatel s uživatelským oprávněním je zaměstnanec, k výkonu jehož práce je nezbytné používání výpočetní techniky a programů.
3. Výpočetní techniku a programy jsou oprávněni používat pouze zaměstnanci s uživatelským účtem, a to v rozsahu svého uživatelského oprávnění
4. Zaměstnancům je zakázáno:
    a. poškozovat výpočetní techniku, programy nebo data nesprávným nebo neoprávněným užíváním
    b. používat výpočetní techniku, programy nebo data protiprávním způsobem nebo k protiprávní činnosti

c. používat výpočetní techniku, programy nebo data k činnostem namířeným proti škole či proti jakémukoliv jinému subjektu, jehož počítačové prostředky jsou dostupné prostřednictvím sítě nebo prostřednictvím internetu
d. umožnit přístup k výpočetní technice, programům nebo datům osobám, které nejsou oprávněnými uživateli podle této směrnice,
e. používat elektronické informace a data, k nimž nemají oprávněný přístup,
f. používat elektronické informace a data, k nimž mají oprávněný přístup způsobem, který je v rozporu s platnými právními předpisy nebo v rozporu s vnitřními předpisy školy,
g. kopírovat neoprávněně programy nebo jejich části,
h. modifikovat neoprávněně programy a data,
i. odposlouchávat neoprávněně provoz (komunikaci) v síti a vytvářet kopie elektronických informací či dat procházejících jednotlivými uzly sítě,

5. Zaměstnanec je však povinen respektovat, že soukromé záležitosti lze v pracovní době a na pracovišti vyřizovat pouze výjimečně v přiměřené a nezbytné míře a nesmí tím být dotčeno plnění povinností zaměstnance podle právních předpisů a podle vnitřních předpisů školy.
6. Zaměstnavatel je oprávněn v případě vážného důvodu nebo úniku osobních údajů nebo řešení jiného bezpečnostního incidentu, kontrolovat elektronickou poštu.

Čl 12. Bezpečnostní pravidla uživatelů

Zaměstnanci jsou povinni dodržovat následující bezpečnostní pravidla při zpracovávání osobních údajů:

1. Svěřenou výpočetní techniku využívají pouze pro plnění pracovních povinností.
2. Dodržují zásady pro tvorbu přístupového hesla k operačním systémům a/nebo aplikacím.
3. Zachovávají jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělují a nikde a nijak si jej nezaznamenávají.
4. Při přihlašování k operačním systémům nebo aplikacím dbají na to, aby nebylo možné heslo odpozorovat další osobou.
5. V případě jakéhokoliv podezření na kompromitaci hesla nebo dokonce jeho zneužití heslo okamžitě změní.
6. Před opuštěním pracoviště zabezpečují výpočetní techniku uzamčením pracovní plochy nebo odhlášením (např. pomocí kláves ⊞+L nebo ctrl+alt+del).
7. Dodržují pravidlo „prázdného stolu“, to znamená, že všechny dokumenty obsahující osobní údaje, které v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních.
8. Při používání přenosné výpočetní techniky a datových nosičů (notebooků, flash disků, externích HDD, DVD apod.) mimo prostory organizace:
    a. nepředávají tuto techniku a nosiče třetím osobám,

   b. učiní všechna dostupná opatření, která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávají je bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.),
   c. nepoužívají výpočetní techniku na veřejných místech pro práci s daty organizace,
   d. ztrátu či odcizení okamžitě nahlásí svému nadřízenému.
9. Neinstalují software na výpočetní techniku organizace.
10. Nepoužívají soukromé datové nosiče (např. CD, flash disky, externí HDD).
11. Nenavštěvují rizikové internetové stránky.
12. Důsledně ověřují doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), takovou zprávu neotvírají, nereagují na ní a tuto skutečnost neprodleně ohlásí správci ICT.
13. Nezasahují do výpočetní techniky a její konfigurace, vyjma situací, kdy toto bude vyžadováno přímo správcem ICT.
14. Odpovídají za zálohování dat na přidělené výpočetní technice.
15. Nekopírují, neukládají, nepřenáší osobní údaje a data z aplikací organizace na pevných discích počítačů, jiných datových nosičích či cloudu, vyjma stanovených úkolů a povinností či po schválení ředitelem organizace.
16. Soubory, obsahující osobní údaje, adresované mimo doménu školy, zasílat pouze chráněné (prostřednictvím datových schránek, nebo prostřednictvím elektronické pošty minimálně v archivním souboru (např. ve formátu „zip“, „rar“ atd.) opatřeného heslem, přičemž heslo zaslat adresátovi jiným komunikačním kanálem, např. prostřednictvím SMS).
17. Soubory, obsahující zvláštní kategorie osobních údajů, zasílat pouze prostřednictvím datové schránky.
18. Netisknou data z aplikací organizace pro jiné než pracovní účely.
19. Pokud dojde k úniku, kompromitaci nebo ztrátě dat obsahujících osobní údaje je každý zaměstnanec povinen neprodleně hlásit tento incident nadřízenému vedoucímu zaměstnanci, který tuto skutečnost hlásí neprodleně pověřenci pro ochranu osobních údajů.

<u>Zaměstnanci mají vysloveně zakázáno:</u>

1. sdělovat někomu své uživatelské jméno a heslo do PC, do počítačové sítě, školní matriky a pracovní emailové adresy, jiných informačních systémů školy. Dále pak je zakázáno sdělovat přístupové údaje do administrace webových stránek a sociálních sítí, pokud jej k tomu nevyzve ředitel školy pro pracovní účely, tj. zaměstnanec nemůže udělovat přístupové údaje oprávnění k administraci nebo editaci komukoliv bez povolení ředitele školy.
2. zasahovat do instalace počítačových programů, měnit konfiguraci, příkazové soubory nebo adresáře potřebné pro chod systému

3. jakkoliv šířit kterýkoliv počítačový program a používat či poskytnout jakékoliv neoprávněné získané prostředky (licenční kódy, hardwarové klíče) slouží k ochraně počítačových programů
4. provádět nezodpovědnou nebo dokonce zlomyslnou činnost na internetu (rozesílání spamu, šíření virů
5. komunikovat se subjekty údajů (zákonní zástupci žáků) ze soukromých emailových adres, ačkoliv by si plnili své pracovní povinnosti.

Čl 13. Práce z domova (home office)

1. Při práci z domova je místem výkonu práce pro zaměstnance jejich bydliště či jiné zvolené místo. Změna místa výkonu práce se provádí písemnou dohodou výkonu práce z domova obou smluvních stran nebo dodatkem obsahu pracovní smlouvy.
2. Doba trvání práce z domova je vykonávaná dle § 184 a), školského zákona a § 317 zákoníku práce.
3. Dohoda o práci z domova je vždy stanovena mezi zaměstnavatelem a zaměstnance.
4. <u>V rámci plnění pracovních povinností je zaměstnanec povinen:</u>
    a. Účastnit se on-line způsobem školení zaměstnavatele v oblasti GDPR
    b. Účastnit se online pracovních porad, webinářů a jiných aktivit pro plnění pracovních povinností
    c. U pedagogických pracovníků se vyžaduje účast na provádění distančního vzdělávání (dětí, žáků, studentů)
    d. Zabezpečit důvěrnost veškerých osobních údajů s žáky a jiných informací zpracovaných v souvislosti s výkonem práce z domova
    e. Zamezit přístupu neoprávněných osob k užívaným pracovním prostředkům a zpracovaných údajů
    f. Se svěřenými prostředky ze strany školy v případě zápůjčky řádně hospodařit, ochraňovat před ztrátou, poškozením, zničením a zneužitím
    g. Předávat zaměstnavateli údaje pro evidenci pracovní doby
    h. V případě úniku osobních údajů informovat ředitele školy
5. Při práci z domova je na dohodě zaměstnavatele se zaměstnancem jaké IT zařízení bude pro plnění pracovních úkolů využívat. V případě využití však svého soukromého IT zařízení je nutné, aby výpočetní a telekomunikační technika měla odpovídající software, který bude mít prvky technického zabezpečení. Náklady na pořízení takového software jsou však v režii zaměstnance, nikoliv zaměstnavatele. V případě zapůjčení IT techniky ze strany zaměstnavatele, zaměstnanci dochází k uzavření dohody o odpovědnosti za ztrátu svěřených předmětů ve smyslu § 255 zákoníku práce a písemného potvrzení o převzetí hodnot.

Zaměstnanci mají právo a povinnosti:

1. mít přístup ke svému PC a nainstalovaným počítačovým programům, které potřebují k pracovním účelům.
2. požadavky na konzultace, instalace, nastavení či opravy sdělovat řediteli školy, který se obrátí na správce IT nebo koordinátora ICT.
3. předkládat řediteli školy požadavky nebo nákup programů zabezpečení PC, které je v majetku školy.
4. IT zařízení, které využívá zaměstnanec nebo více zaměstnanců k pracovním účelům vždy odhlásit před odchodem z pracoviště, i při přerušení práce, pokud zůstane IT zařízení na pracovišti nezamčeném nebo s přístupem více osob.
5. po ukončení práce vypnout IT zařízení alespoň elektronicky do stavu stand- by
6. v případě toho, že nebudete na IT zařízení delší dobu pracovat, je potřeba toto zařízení vypnout mechanicky.
7. zachovávat mlčenlivost o údajích obsažených v souborech, v databázích či v informačních systémech a o všech dalších skutečnostech, o nichž se dozvědí v souvislosti s výkonem práce v rámci pracovního poměru ve škole; o těchto skutečnostech jsou povinni zachovávat mlčenlivosti po skončení pracovního poměru práce ve škole.;
8. zachovávat mlčenlivost o osobních údajích, včetně údajů citlivých, a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů;
9. výše uvedené skutečnosti a údaje nesdělovat třetím osobám, nedovolit přístup
10. neoprávněných osob k těmto údajům, neohrozit ztrátu těchto údajů;
11. skutečnosti chráněné školským zákonem (§ 28) a osobní údaje zpracovávat jen se souhlasem zaměstnavatele a za účelem, který zaměstnavatel stanoví
12. zachovávat důvěrnost obsahu veškeré elektronické komunikace a obsahu databází;
13. dodržovat závazek mlčenlivosti, zachovávat mlčenlivost o všech informacích, se kterými přijdou během svého pracovního poměru práce do styku; toto je závazné i po skončení pracovního poměru
14. být si vědomi, že porušení výše uvedených povinností je závažným porušením pracovních povinnosti;
15. být si vědomi, že zaměstnavatel je po nich oprávněn vymáhat případnou škodu, kterou porušením výše uvedených povinností způsobí.

Čl 14. Práva a povinnosti Správce ICT

Správce ICT

Správce ICT je zodpovědný za dodržování bezpečnostních pravidel při zpracovávání a ochraně osobních údajů v rámci počítačové sítě a na výpočetní technice organizace. Je povinen dodržovat následující bezpečnostní pravidla při plnění pracovních úkolů správce ICT:

1. Spolupracuje s organizací na tvorbě a aktualizaci analýzy rizik.

2. Spravuje antivirový systém na všech výpočetních prostředcích organizace a to především:
    a. provádí jeho instalaci,
    b. kontroluje funkčnost aktualizací,
    c. kontroluje výstupy programu.
3. Pro zaměstnance organizace připravuje a instaluje výpočetní techniku, kterou nastaví dle definovaných bezpečnostních požadavků (např. způsoby přihlášení, oprávnění uživatelského účtu, uzamykání počítače při neaktivitě apod.) a následně ji předává určeným zaměstnancům k použití.
4. Vytváří a nastavuje zaměstnancům uživatelská oprávnění do počítačové sítě a aplikací v rozsahu schváleném ředitelem.
5. Na základě požadavku ředitele organizace zřizuje nebo ruší přístupy do operačních systémů organizace.
6. Na základě požadavku garanta aplikace zřizuje nebo ruší přístupy do aplikace organizace.
7. Zajišťuje fyzickou bezpečnost datových úložišť, nosičů a dat organizace.
8. Poskytuje zaměstnancům organizace technickou podporu při využívání výpočetní techniky.
9. Provádí kontrolní činnost k zajištění bezpečnosti osobních údajů zpracovávaných ve výpočetní technice organizace.
10. Vede provozní deník, ve kterém zaznamenává všechny klíčové činnosti související se správou počítačové sítě organizace.
11. Provádí bezpečnou likvidaci datových nosičů organizace, zejména pak pevných disků, flash disků, paměťových karet, CD a DVD disků apod.
12. V případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení, V případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení,
13. likvidace apod.), musí před odesláním vymazat z pevného disku veškeré osobní údaje nebo musí vyjmout paměťová média.
14. Provádí zálohování zpracovávaných dat a klíčových síťových prostředků organizace tak, aby při selhání např. hlavního datového úložiště, bylo možné provést obnovu dat s minimální ztrátou uložených dat.

Správce ICT má právo:

1. přistupovat na IT zařízení uživatele za účelem údržby či opravy pod přihlášením administrátora;
2. upřednostňovat práce, které jsou v obecném zájmu školy (počítačová síť) před prací na jednotlivých pracovištích (lokální PC);

3. zvolit způsob vyřízení požadavku po zvážení všech technických variant a s přihlédnutím k finanční a časové rentabilita;
4. odmítnout nestandardní požadavky uživatelů, které např. nejsou v zájmu školy, nejsou odůvodněné, nejsou technicky nebo licenčně čisté apod.

Čl 15. Bezpečnost sítě

1. V případě, že organizace provozuje Wi-Fi síť, je potřeba dodržovat určitá bezpečnostní pravidla. Wi-Fi síť organizace je používána jen pro přístup do sítě Internet. Je chráněna standardními prostředky včetně přístupového hesla. Heslo pro přístup do sítě Wi-Fi je pravidelně měněno 1x za 12 měsíců.
2. V nastavení přístupových údajů k administraci routerů musí odpovědná osoba změnit továrně nastavené přístupové údaje. Kvalita nového hesla splňuje požadavky pro heslo správce ICT.
3. Mobilní zařízení organizace (smartphony, tablety) s vlastním operačním systémem jsou vybavena antivirovou aplikací.
4. Zaměstnanci mohou využívat soukromá mobilní zařízení pouze pro práci s obsahem pracovní emailové schránky. Jiné využití soukromých mobilních zařízení pro pracovní účely (např. připojení do vnitřní sítě organizace, administrace aplikací apod.) je zakázáno.
5. Pokud je Wi-Fi síť používána pro přístup k interní síti, a tedy i aplikacím organizace, je identita zaměstnance před zpřístupněním této sítě ověřena prostřednictvím zadání přístupových údajů. Bez ověření identity zaměstnance nejsou interní síť, aplikace nebo síťové disky zpřístupněny.
6. Přístup k zálohám síťových prostředků a síťovým aplikacím je striktně omezen jak na logické, tak i fyzické úrovni pouze na odpovědné osoby.
7. Všechny vzdálené přístupy k síti organizace (pomocí např. vzdálené plochy nebo VPN) povoluje ředitel.
8. <u>Všechny způsoby vzdáleného přístupu k síti organizace splňují následující:</u>
    a. vytvořené spojení v rámci vzdáleného přístupu je šifrované (bez ohledu na povahu přenášených dat) a předchází mu autentizace (minimálně heslem, lépe uživatelským certifikátem),
    b. každý vzdálený přístup je jednoznačně identifikovatelný (uživatel) a je zaznamenán,
    c. uživatelé nesmí „propůjčovat“ své oprávnění vzdáleného přístupu třetím osobám, byť zaměstnancům organizace,
    d. připojení probíhá prostřednictvím bezpečného kanálu (HTTPS, VPN, pomocí VPN mimo veřejnou síť poskytovatele apod.).
    e. Správce ICT vede evidenci zaměstnanců a výpočetní techniky s povoleným vzdáleným přístupem. Tyto seznamy jsou v pravidelných intervalech (alespoň

jedenkrát za rok) přezkoumávány ředitelem organizace, nebo jím pověřenou osobou.

9. V případě, že Správce ICT nastavuje samostatné segmenty sítě, jako jsou např. servery, síťové tiskárny, zasedací místnosti apod, síťové zásuvky organizace jsou připojeny dle jejich využití. Nepoužívané zásuvky jsou správcem ICT v rozvaděči odpojeny.
10. Správce ICT přezkoumává v pravidelných intervalech (alespoň 1x za měsíc) důležité bezpečnostní logy firewallu. Například využití sítě (jednotlivých portů), neúspěšné pokusy o vzdálené přihlášení, pokusy o skenování sítě apod.

Čl 16. Používání výpočetní techniky

1. Uživatel je oprávněn užívat pouze výpočetní techniku, která mu byla řádně předána, nebo jejíž užívání má zpřístupněno prostřednictvím výpočetní techniky, která mu byla řádně předána (např. sdílené notebooky, tiskárny).
2. Výpočetní techniku je zaměstnanec oprávněn užívat pouze k činnostem souvisejícím s jeho prací a pouze v souladu s příslušným návodem k danému zařízení výpočetní techniky.
3. Pokud jde o technickou manipulaci s výpočetní technikou, je uživatel oprávněn pouze k běžným uživatelským činnostem jako např. výměna toneru, cartridge, doplnění papíru v tiskárně, připojení k síti a odpojení od sítě. Uživateli je zakázáno rozpojovat nebo přerušovat počítačovou síť, připojovat poprvé k síti nové PC nebo jiná technická nařízení. Manipulace s výpočetní technikou, které nesmí provádět uživatel, zabezpečuje správce sítě.
4. Závadu ve funkčnosti výpočetní techniky je uživatel povinen neprodleně oznámit správci sítě. Veškeré opravy výpočetní techniky zabezpečuje pouze správce sítě.
5. Uživatel nesmí provádět změny konfigurace PC, jiných zařízení nebo zásahy do systému, které by mohly vést k jeho zhroucení, poruše nebo nežádoucímu chování. Jakékoliv nestandardní zásahy do konfigurace nebo systému je nutné předem projednat se správcem sítě.
6. Do sítě je zakázáno bez souhlasu správce nebo nadřízeného pracovníka, přímo nebo nepřímo připojovat jakákoliv technická zařízení, která uživatel nemá schválená k užívání.
7. Do PC je zakázáno připojovat přenosné a externí diskové jednotky včetně USB flash disků kromě zařízení schválených správcem sítě nebo nadřízeného pracovníka.
8. Obdrží-li uživatel (na přenosném médiu, elektronickou poštou či jiným způsobem) jakýkoliv soubor z neznámé adresy, nebo o jehož původu lze důvodně pochybovat, je zakázáno soubor otevírat či ukládat na disk. Rovněž je zakázáno spouštět bez předchozí konzultace se správcem sítě spustitelné soubory došlé na přenosném médiu nebo elektronickou poštou, zejména pak soubory s koncovkami *.exe, *.com, *.bat, *.pif, *.vbs, *.vbe.

9. Má-li uživatel podezření na napadení PC virem, neprodleně informuje správce sítě.
10. Uživatel je oprávněn využívat pouze ta přístupová práva, která mu byla řádně přidělena. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla řádně přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci sítě a takto neoprávněně získaná přístupová práva náležející jinému uživateli; na pracovištích s výpočetní technikou užívanou společně více uživateli, je možné společné užívání je možné společné užívání přístupových práv, pokud byla takto stanovena.
11. Elektronické informace a data přístupná prostřednictvím výpočetní techniky a sítě může uživatel využívat pouze, je-li k tomu oprávněn v rámci výkonu své práce a je-li to pro výkon jeho práce nezbytné. Uživatel je povinen při nakládání s daty dodržovat všechny související právní předpisy.
12. Škola si vyhrazuje právo v odůvodněných případech v souladu s právními předpisy monitorovat dobu přístupu jednotlivých zaměstnanců na internetové stránky, včetně adres těchto stránek a dále právo monitorovat u jednotlivých zaměstnanců počty došlých a odeslaných e-mailů, včetně adres odkud nebo kam je e-mail směrován. Se zjištěnými údaji musí být nakládáno v souladu s ochranou soukromí a ochranou osobních údajů.
13. Zaměstnanec musí v případě využití IT techniky, které není v majetku školy, zabezpečit toto zařízení při používání internetu neb jiných aplikací, využívání neautorizovaných internetových portálů a neoriginálních software tak, aby nedocházelo k úniku osobních údajů nebo jiných bezpečnostních incidentů.

Čl 17. Závěrečná ustanovení

1. Vnitřní předpis je zaměstnancům k dispozici ve sborovně školy
2. Všichni vedoucí zaměstnanci školy jsou povinni seznámit své podřízené zaměstnance, včetně osob pracující pro školu na základě DPP nebo DPČ.
3. Tato směrnice nahrazuje Směrnici o ochraně osobně údajů ze dne 25.5.2018

_____

Mgr. Tomáš Daněk

ředitel