GYMNÁZIUM, ÚSTÍ NAD LABEM, JATEČNÍ 22, PŘÍSPĚVKOVÁ ORGANIZACE					
OCHRANA OSOBNÍCH ÚDAJŮ					**V9**
VNITŘNÍ SMĚRNICE		SPISOVÝ ZNAK	1.11	ÚČINNOST	3. 4. 2023
VYPRACOVALA	MGR. NIKOLA VODIČKOVÁ				
REVIDOVALA	MGR. MARTINA LANDOVÁ	SKARTAČNÍ ZNAK	A	Č. J.	GJ/1436/2023

ČLÁNEK 1
ÚVODNÍ USTANOVENÍ

1.1 Tato směrnice upravuje postupy správce, jeho zaměstnanců, případně dalších osob při nakládání s osobními údaji, pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů. Směrnice rovněž upravuje některé povinnosti správce, jeho zaměstnanců, případně dalších osob při nakládání s osobními údaji.

1.2 Tato směrnice je závazná pro všechny zaměstnance správce. Směrnice je závazná i pro další osoby, které mají se školou jiný právní vztah a které se zavázaly postupovat podle této směrnice.

ČLÁNEK 2
VYMEZENÍ POJMŮ

Správce: Gymnázium, Ústí nad Labem, Jateční 22, příspěvková organizace
Pověřenec: pověřenec pro ochranu osobních údajů, se kterým škola spolupracuje na základě nařízení GDPR.
Pojmy vztahující se k problematice osobních údajů jsou definovány identicky s nařízením GDPR.

ČLÁNEK 3
ZÁSADY NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

Při nakládání s osobními údaji se správce, jeho 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, při ochraně oprávněných zájmů správce, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,
e) respektovat práva člověka, který je subjektem údajů, zejména práva udělit a odvolat souhlas se zpracováním, práva na výmaz, namítat rozsah zpracování apod.,
f) poskytovat při zpracování osobních údajů zvláštní ochranu citlivým údajům,
g) poskytovat informace o zpracování osobních údajů,
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.

ČLÁNEK 4
POSTUPY SPRÁVCE, JEHO ZAMĚSTNANCŮ A DALŠÍCH OSOB PŘI NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

3.1 Správce všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Přitom správce 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 statutárnímu zástupci správce známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením statutárního zástupce správce.

3.2 Správce zavede taková opatření, aby o nakládání a zpracování osobních údajů měl přehled alespoň pověřenec správce nebo jím pověřená osoba. 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 správce uzavírá se třetí osobou (nájemní smlouva, smlouva o dílo, smlouva o poskytování služeb).

3.3 Správce alespoň jednou za půl roku provede zhodnocení postupů při nakládání a zpracování osobních údajů, a to formou průběžného auditu. Zjistí-li se, že některé postupy správce jsou zastaralé, zbytečné nebo se neosvědčily, učiní správce bezodkladně nápravu.

3.4 Každý zaměstnanec správce 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. Zaměstnanec zejména osobní údaje nezveřejňuje bez ověření, že takový postup je možný, nezpřístupňuje osobní údaje osobám, které neprokáží právo s nimi nakládat. Zaměstnanec, vyplývá-li taková povinnost z jiných dokumentů, informuje subjekt údajů o jeho právech na ochranu osobních údajů; případně odkáže na ředitele správce nebo na pověřence.

3.5 Správce při nakládání a zpracovávání osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů. Povinnosti pověřence vyplývají z nařízení GDPR a dále pak ze smlouvy uzavřené s pověřencem.

3.6 Správce ihned řeší každý bezpečnostní incident týkající se osobních údajů, a to v součinnosti s pověřencem. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, správce tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepíše záznam. Statutární zástupce správce a pověřenec posuzují závažnost bezpečnostního incidentu z pohledu jeho hlášení Úřadu pro ochranu osobních údajů. O každém závažném incidentu informuje správce prostřednictvím pověřence Úřad pro ochranu osobních údajů.

3.7 Správce shromažďuje žádosti o osobní údaje prostřednictvím pro tyto účely zřízené e-mailové schránky gdpr@gymjat.cz.

ČLÁNEK 5
ORGANIZAČNÍ OPATŘENÍ K OCHRANĚ OSOBNÍCH ÚDAJŮ VE ŠKOLE

4.1 Veškeré listiny, které obsahují osobní údaje, jsou trvale uloženy v uzamykatelných skříních či prostorách v kanceláři oprávněných osob (specifikováno ve vstupní bezpečnostní analýze vyhotovené správcem). Ostatním zaměstnancům jsou zapůjčeny na nezbytně dlouhou dobu k provedení činností pro stanovený účel. Tyto listiny nelze vynášet z prostor správce, předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.

4.2 Veškeré elektronické dokumenty, které obsahují osobní údaje, jsou vedeny/uloženy vždy v zabezpečeném informačním systému (specifikováno ve vstupní bezpečnostní analýze vyhotovené správcem). Do všech informačních systémů mají přístup jednotliví zaměstnanci správce jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením (dále jen „oprávněné osoby“). Při práci s informačním systémem 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 správce, který nastavuje potřebné zabezpečení dat a počítačové sítě (dle pokynů statutárního zástupce správce).

4.3 Elektronický přístup k osobním údajům se řídí aktuální verzí dokumentu “Doporučené standardy a úroveň zabezpečení v oblasti IT”, který vyhotovil pověřenec, a bude v pravidelných intervalech aktualizován.

4.4 Zaměstnanci správce neposkytují bez právního důvodu žádnou formou osobní údaje zaměstnanců správce a/nebo jiných osob cizím osobám a institucím, tedy ani telefonicky ani mailem ani při osobním jednání. O zpřístupnění osobních údajů třetím osobám a institucím na základě jejich písemné žádosti sepíší záznam o zpřístupnění osobních údajů (např. soud, exekutor, policie).

4.5 Listiny, které se odesílají mimo prostory správce, např. pro potřeby daňového řízení, soudního řízení, správního řízení, zpracovávají zaměstnanci určení statutárním zástupcem správce nebo v rámci svých pracovních povinností. Tyto listiny musí být vždy přepravovány obezřetně tak, aby se při jejich manipulaci předešlo neoprávněnému zpřístupnění osobních údajů (např. v případě jejich odesílání v rámci poštovní přepravy se odesílají v neprůhledných obalech a řádně uzavřené).

4.6 V propagačních materiálech správce, ve výroční zprávě, na webu či na jiných veřejně přístupných místech lze po dohodě s dotčenými osobami uveřejňovat jejich osobní údaje ve sjednaném rozsahu.

4.7 Uzavírá-li správce jakoukoli smlouvu, k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, které správce zpracovává, bude správce vždy a bezpodmínečně 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, opatření musí být na minimálně stejné či vyšší úrovni zabezpečení osobních údajů jako má nastaven primární správce údajů,
b) nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu správce,
c) zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,
d) zajistit, aby 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 správci bez zbytečného odkladu nápomocen při plnění povinností správce, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů, povinnosti posoudit vliv na ochranu osobních údajů a povinnosti provádět předchozí konzultace, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje správce,
f) po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí správci a vymaže existující kopie apod.,
g) poskytnout správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené správci právními předpisy,
h) umožnit kontrolu, audit či inspekci prováděné správcem nebo příslušným orgánem dle právních předpisů,
i) poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví správce, součinnost potřebnou pro plnění zákonných povinností správce spojených s ochranou osobních údajů, jejich zpracováním,
j) poskytnuté osobní údaje chránit v souladu s právními předpisy,
k) přiměřeně postupovat podle této směrnice, která je přílohou smlouvy.

4.8 Správce provozuje kamerové systémy výhradně za účelem ochrany majetku, nikoliv sledování zaměstnanců nebo jiných osob. Kamerové záznamy snímají pouze společné prostory školy a prostory, které byly identifikovány jako potenciálně rizikové vzhledem ke vniknutí nepovolaných osob do prostor školy. Záznamy z kamerového systému jsou uchovávány maximálně po dobu 7 dní a následně jsou smazány (pokud neexistuje vážný důvod pro ponechání daného konkrétního záznamu – např. jako důkaz pro policii při podezření na spáchání trestného činu / přestupku).

ČLÁNEK 6
SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

5.1 Ke zpracování osobních údajů nad rozsah vyplývající ze zákonů (případně dalších důvodů stanovených legislativou) je nezbytný souhlas osoby, o jejíž osobní údaje se jedná. Souhlas musí být informovaný a konkrétní, nejlépe v písemné podobě. Souhlas se získává pouze pro konkrétní údaje (určené např. druhově), na konkrétní dobu a pro konkrétní účel.

5.2 Souhlas se poskytuje vždy na předem definovanou dobu a účel. Udělený souhlas může být v souladu s právními předpisy odvolán.

ČLÁNEK 7
NĚKTERÉ POVINNOSTI SPRÁVCE, JEHO ZAMĚSTNANCŮ A DALŠÍCH OSOB PŘI NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

6.1 Každý zaměstnanec správce je povinen počínat si tak, aby neohrozil ochranu osobních údajů zpracovávaných správcem.

6.2 Dále je každý zaměstnanec správce povinen

a) zamezit nahodilému a neoprávněnému přístupu k osobním údajům, které správce zpracovává,

b) pokud zjistí porušení ochrany osobních údajů, neoprávněné použití nebo zneužití osobních údajů nebo jiné neoprávněné jednání související s ochranou osobních údajů, bezodkladně zabránit dalšímu neoprávněnému nakládání, zejména zajistit znepřístupnění a ohlásit tuto skutečnost statutárnímu zástupci správce a pověřenci.

6.3 Statutární zástupce správce je povinen

a) vyhotovit a pravidelně aktualizovat bezpečností analýzu zpracovaní osobních údajů u správce, zejména z pohledu shromažďovaných osobních údajů, oprávněných osob a zabezpečení osobních údajů,

b) informovat zaměstnance o všech významných skutečnostech, postupech nebo událostech souvisejících s nakládáním s osobními údaji u správce, a to bez zbytečného odkladu,

c) zajistit, aby zaměstnanci správce byli řádně poučeni o právech a povinnostech při ochraně osobních údajů,

d) zajišťovat, aby zaměstnanci správce byli podle možností a potřeb správce vzděláváni nebo proškolováni o ochraně osobních údajů

e) zajistit, aby správce byl schopen řádně doložit plnění povinností správce při ochraně osobních údajů, které vyplývají z právních předpisů.

ČLÁNEK 8
ZÁVĚREČNÁ USTANOVENÍ

(1) Tento vnitřní předpis nabývá účinnosti dnem 3. 4. 2023.

(2) Zrušuje se směrnice Ochrana osobních údajů V4-18 ze dne 25. 5. 2018.

(3) Kontakt na pověřence školy: Mgr. Martina Landová, mart.landova@seznam.cz, DEVELOP Most.

V Ústí nad Labem 3. 4. 2023

.....
Mgr. Radka Brejchová
ředitelka

Přílohy:

PŘÍLOHA Č. 1 - DOPORUČENÉ STANDARDY A ÚROVEŇ ZABEZPEČENÍ V OBLASTI IT

PŘÍLOHA Č. 2 - ZÁZNAM O ZPŘÍSTUPNĚNÍ OSOBNÍCH ÚDAJŮ

PŘÍLOHA Č. 1 - DOPORUČENÉ STANDARDY A ÚROVEŇ ZABEZPEČENÍ V OBLASTI IT

1/ Přístup k osobním údajům

Doporučené zabezpečení osobních údajů podle jejich způsobu uložení	
Osobní údaje jsou uloženy přímo na pevném disku daného počítače	● počítač musí být přístupný pouze na heslo/uživatelské jméno, které je individuální pouze pro osobu oprávněnou k přístupu k osobním údajům (tj. nikoliv např. sdílené heslo pro všechny učitele) ● počítač musí být v době, kdy je nepoužívaný/vypnutý, v uzamčené místnosti
Osobní údaje jsou uloženy na serveru (ve sdílené složce) – tedy potenciálně dostupné z jakéhokoliv počítače ve školní síti	● musí být zajištěno, že osobní údaje jsou dostupné pouze oprávněným osobám (tj. do sítě je potřeba se hlásit na konkrétní uživatelský účet / jméno nebo složka musí být dostupná pod heslem, které je známé pouze příslušné oprávněné osobě), zároveň vyžadujeme dvoufázové ověření ● server by měl být ve speciální zamčené místnosti s přístupem pouze pro nezbytný okruh osob (ředitel, IT technik) ● data na serveru by měla být šifrovaná
Osobní údaje jsou uloženy v cloudu (potenciálně dostupné z jakéhokoliv počítače či mobilního zařízení)	● všechny počítače či mobilní zařízení, která jsou využívána pro přístup k osobním údajům, musí být řádně zabezpečena - musí vyžadovat heslo pro přístup ● přístup k souborům by měl být chráněn heslem, které je potřeba zadat při každém novém přihlášení do cloudové služby (tj. nikoliv „zapamatovat heslo") ● je potřeba mít s poskytovatelem cloudové služby uzavřenou dohodu/smlouvu dle požadavků GDPR
Osobní údaje jsou uloženy ve speciálním software (např. Bakaláři, Škola online, účetní systémy apod.)	● všechny počítače či mobilní zařízení, které jsou využívány pro přístup k osobním údajům, musí být řádně zabezpečeny – musí vyžadovat heslo pro přístup ● systém by měl umožňovat individualizovaný přístup pro jednotlivé uživatele a nastavení práv tak, aby bylo možné nastavit každému práva pouze na určitou oblast (tj. nikoliv jedno společné heslo a přístup pro všechny) ● je potřeba mít s poskytovatelem systému uzavřenou dohodu/smlouvu dle požadavků GDPR

Obecná doporučení ke všem typům uložení osobních údajů

- osobní údaje je potřeba ukládat pouze do složek a programů k tomu určených - nelze např. přenášet na flash-disku v nezabezpečené podobě
- při zasílání e-mailem doporučujeme soubor zaheslovat a heslo sdělit příjemci jinou cestou (např. formou SMS)
- při každém opuštění počítače, na kterém probíhá práce s osobními údaji, musí dojít k jeho „uzamknutí" tak, aby při návratu k počítači bylo nutné opět zadat heslo
- ať už se jedná o přístup do počítačové sítě, nebo do speciálního software, zajistí individualizované osobní účty transparentnost v nakládání s osobními údaji – v případě úniku dat se dá vysledovat k jakému konkrétnímu pochybení došlo (pokud přistupují všichni pod jedním účtem / heslem – je jakékoliv vysledování příčiny problému téměř nemožné)
- používat svěřené zařízení digitální techniky pouze pro pracovní účely (tj. nestahovat soubory pro soukromé účely (např. filmy, dokumenty apod.) na disk počítače

2/ Doporučení k tvorbě hesel

- heslo musí obsahovat minimálně 8 znaků
- mělo by se jednat o kombinaci velkých a malých písmen a čísel nebo speciálních znaků
- neměla by obsahovat „slovníková" slova - např. „Skola123"

- měla by být nastavena pravidelná změna hesel, minimálně 2 x za rok (konkrétní dobu stanoví správce údajů)
- hesla by se neměla psát nikam na papír a ukládat poblíž počítače
- heslo pro přístup do počítače by mělo být jiné než heslo pro přístup do softwaru/aplikace s osobními daty (tak, aby se pro přístup k osobním datům zadávala minimálně 2 různá hesla)
- jakýkoliv systém by měl umožnit změnu hesla ze strany uživatele v jakýkoliv okamžik

3/ Aktualizace softwaru

- na počítačích je potřeba mít nainstalované pouze legální verze veškerého softwaru
- je nutné vždy mít software aktualizovaný, zejména
    - operační systém (aktualizuje se většinou automaticky)
    - kancelářský software, např. MS Office (aktualizuje se rovněž automaticky)
    - antivirový program a firewall
    - webový prohlížeč
    - software používaný pro práci s osobními údaji

4/ Předávání / zasílání osobních údajů

- osobní údaje předávané / zasílané v elektronické podobě by měly být vždy zabezpečené / zaheslované tak, aby v případě ztráty média (např. flash-disk) nebo nabourání se do emailu nebylo možné se k osobním údajům dostat bez znalosti přístupového hesla
- osobní údaje nelze posílat přímo v těle e-mailu / zprávy, ale formou zaheslované přílohy
- nejlépe je zasílat osobní údaje formou datové schránky

5/ bezdrátová síť – wifi

- nedoporučujeme používat wifi zcela nezabezpečenou / bez hesla
- minimální způsob zabezpečení je přístup do zabezpečené sítě přes heslo, které je dostupné pouze zaměstnancům a žákům školy
- heslo by se mělo pravidelně měnit – minimálně 1x ročně

6/ správa počítačové sítě

- podle rozsahu počítačové sítě by měla škola zajistit dostatečně kvalitní správu sítě tak, aby byly zajištěny potřebné činnosti (správa a nastavení uživatelských účtů, aktualizace softwaru, nastavení serveru apod.)

Revidovala: Mgr. Martina Landová, pověřenec pro ochranu osobních údajů
Dne: 3. 4. 2023

PŘÍLOHA Č. 2 - ZÁZNAM O ZPŘÍSTUPNĚNÍ OSOBNÍCH ÚDAJŮ

Správce je povinen chránit osobní údaje dotčených osob a je oprávněn je zpřístupnit jen se souhlasem dotčených osob nebo na základě a v souladu s právními předpisy.
Na správce ***Gymnázium, Ústí nad Labem, Jateční 22, příspěvková organizace*** se obrátila osoba:

Jméno a příjmení: _____

datum narození / jiný identifikátor (číslo průkazu): _____

ze společnosti / veřejné instituce_____

se sídlem: _____

se žádostí o zpřístupnění osobních údajů o dotčené osobě:

Jméno a příjmení: _____

datum narození / jiný identifikátor (číslo průkazu): _____

v rozsahu (nebo přiložte žádost):

_____

_____

_____

_____

Z právního důvodu (nebo přiložte žádost):

_____

_____

Pokud neexistuje žádný zákonný důvod pro zpřístupnění osobních údajů, správce požádal dotčenou osobu, aby souhlasila se zpřístupněním osobních údajů žadateli:
souhlasil / nesouhlasil (škrtněte nehodící se) se zpřístupněním výše uvedených osobních údajů.

_____ _____

Datum Podpis dotčené osoby

Správce požadované osobní údaje zpřístupnil/nezpřístupnil (nehodící se škrtněte)

_____ _____

Datum Podpis správce